ENCIRCLE

EuropeaN Cbrn Innovation for the maRket CLustEr

D5.4 ENCIRCLE Cluster Impact Y4

This publication only reflects the view of the ENCIRCLE Consortium or selected participants thereof. Whilst the ENCIRCLE Consortium has taken steps to ensure that this information is accurate, it may be out of date or incomplete, therefore, neither the ENCIRCLE Consortium participants nor the European Community are liable for any use that may be made of the information contained herein.
This document is published in the interest of the exchange of information and it may be copied in whole or in part providing that this disclaimer is included in every reproduction or part thereof as some of the technologies and concepts predicted in this document may be subject to protection by patent, design right or other application for protection, and all the rights of the owners are reserved.
The information contained in this document may not be modified or used for any commercial purpose without prior written permission of the owners and any request for such additional permissions should be addressed to the ENCIRCLE coordinator.

Dissemination level

PU	Unrestricted PUBLIC Access – EU project	X

Document Information

Grant Agreement n°	**740450**	
Project Title	EuropeaN Cbrn Innovation for the maRket CLustEr	
Project Acronym	ENCIRCLE	
Project Coordinator	Université catholique de Louvain (UCL)	
Document Responsible Partner	Miksei	
Document Number	D5-4	
Document Title	ENCIRCLE Cluster Impact Y4	
Dissemination Level	PU	
Contractual Date of Delivery	Month 49 (March 2021)	

Partners involved in the Document

N°	Participant organisation name (short name)	Check if involved
1	Université Catholique de Louvain (UCL)	X
2	BAE SYSTEMS (BAES)	X
3	Ouvry SAS (OUVRY)	X
4	Sieć Badawcza Łukasiewicz - Przemysłowy Instytut Automatyki i Pomiarów PIAP	X
5	Tecnoalimenti (TCA)	X
6	Wojskowa Akademia Techniczna (WAT)	X
7	European Virtual Institute for Integrated Risk Management (EU-VRi)	X
8	Istituto Affari Internazionali (IAI)	X
9	Université de Nice-Sophia Antipolis (UNS)	X
10	Universita Cattolica del Sacro Cuore (UCSC)	X
11	FALCON COMMUNICATIONS LIMITED (FALCON)	X
12	Smiths Detection Watford Limited (SMITHS)	X
13	MIKKELIN KEHITYSYHTIO MIKSEI OY (MIKSEI)	X
14	ENVIRONICS OY (EOY)	X
15	ADS GROUP LIMITED LBG (ADS)	X

Circulation list

- European Commission
- ENCIRCLE Consortium

Executive Summary

The main goal of the ENCIRCLE Project is to strengthen the European industry to help create the tools and strategies needed to consolidate the EU CBRN communities of suppliers and practitioners in order to strengthen the field of CBRN safety, security and defence in the European Union.

The purpose of this Deliverable D5-4 is to summarise the discussion to date on the ENCIRCLE Project covering the period March 2020 to March 2021 and presents the latest information concerning:

- Innovation Developments
- Status updates on the projects TERRIFFIC, EU-SENSE, COSMIC, SERSING and EU-RADION
- Developments on the ENCIRCLE Catalogue
- Developments on the ENCIRCLE innovation watch and CBRN needs and gaps
- Workshops and Events conducted by ENCIRCLE in year 4
- Market and Business support developments including an updated market analysis
- Integration and technical support concerning standards development and Human Factors

Table of Contents

List of Figures

1 Introduction

The main goal of the ENCIRCLE project is to strengthen the European industry to help create the tools and strategies needed to consolidate the EU CBRN communities of suppliers and practitioners in order to strengthen the field of CBRN safety, security and defence in the European Union.

In order to achieve this goal, an innovative approach was proposed. Based on five objectives, it aims at prompting the innovation and business development, and filling market gaps within the project timeframe. The project objectives include:

- Create an open and neutral EU CBRN cluster
- Provide a sustainable and flexible vision and roadmap for the development of the European CBRN market and innovations
- Provide integration with platforms (systems, tools, services, products) by proposing standardized interfaces and future EU standards to integrate CBRN technologies and innovations developed from the Part b projects
- Support CBRN safety, security and defence commercial and market services
- Improve and facilitate European CBRN dissemination and exploitation

The purpose of this document is to summarise the ‘impact’ of the ENCIRCLE Project to date, covering the period from March 2020 to March 2021.

2 ENCIRCLE Impact

The ENCIRCLE project has been running since the 10th March 2017 and the following sections summarise the impact to date over the period March 2020 to March 2021.

2.1 INNOVATION PLAN AND DISSEMINATION

2.1.1 Part B Call Topics

The starting point for ENCIRCLE catalogues was list of the technologies which were originally identified as gaps in certain functions (based on the STACCATO functions) of the main phases in the CBRN Security Cycle (Prevention, Preparedness, Response, Recovery) at the end of the EDEN project. This catalogue was updated based on the careful evaluation of its content as well as other contributions including workshops in 2017. In the second year of project realisation we have continued work on evaluation of the gaps in the catalogue and focused on their prioritisation. During our work we were supported by practitioners who, during events such as Bio-Garden exercise organised by H2020 project eNOTICE and ESA project B-LIFE, have reviewed full list of needs and gaps. Our efforts have led to development of the draft of the topics catalogue. This catalogue was further extended by addition of comments regarding market pull, standardization and links to EU CBRN Action Plan. The catalogue of needs and gaps has been refined and updated since the project has commenced as follows:

- D3.9 Part B 2017 Call Topics – recommended for the 2017 call, issued in May 2017 – three selected projects in 2017 call included COSMIC, TERRIFFIC and EU-SENSE.
- D3.10 Refined future Part B Call Topics - as a result of the ENCIRCLE workshop in Nov 2018.
- D3.11 Part b 2019 Call Topics - before publishing call the list of the topic was additionally reviewed by the EC and suggested changes and additions have been made. Two selected projects in 2019 call included SERSing and EU-RADION.

In February 2020 we have finalised list of the 9 topics for the last CBRN Cluster call in the H2020 Framework programme, SU-DRS04-2020 CBRN Cluster, which was opened on March 12, 2020. At the beginning of March 2020, this list underwent the final review by the European Commission. In our work on preparation of the list of the topics we have again reviewed carefully list of the needs and gaps and analysed it taking into consideration potential needs fulfilment and gaps closure by the developments of the CBRN-related projects carried out within H2020 Programme. The list of preselected 68 topics was then evaluated and prioritised during consultation process and survey with practitioners.

The survey was conducted using the online survey tool SLIDO, via contact with practitioners' networks, via on-line communications, and presentations at the 21st International CBRN

Symposium 2019 CBRN Internal symposium at in Farnborough and NO-FEAR demonstrations in Rome in May 2019. The survey included responses from the practitioner and technological community from Law enforcement, Fire service, Medical service, Military, Government/public institution, Industry and Academia. The survey was conducted as a multiple choice asking for the participants to respond to what they considered to be the two most important needs that need to be addressed by research and development for implementation in the next five years (the survey received 55 responses). The results of the survey were described in the report "ENCIRCLE 2020 Topic Prioritisation Summary of Survey Results". Based on the results of survey 11 topics with high priority have been identified.

Taking into consideration results of the survey and after a few rounds of the corrections and modifications based on the comments obtained from DG HOME, DG ECHO and REA the list of the topics was reduced to 9. The topics have been clearly linked to EU CBRN Action Plan and were assigned to certain phases in security cycle as well as the threat (CBRNe) they are responding to.

As a result of 2020 CBRN Cluster Part B call European Commission selected two projects for funding, HoloZcan (Deep Learning Powered Holographic Microscopy for Biothreat Detection on Field) and NEST (An interoperable multi-domain CBRN system).

By the end of the ENCIRCLE project duration a final review of the needs and gaps list will be performed. The needs will be linked to EU CBRN Action Plan, assigned to certain phases in security cycle as well as the threat (CBRNe) they are responding to. In addition, EU projects addressing certain needs will be identified and listed. The final list of the needs and gaps will be posted in the ENCIRCLE Dynamic Catalogue.

In addition, the innovation roadmaps for CBRN Cluster Part B projects will be created. By these roadmaps we will attempt to find path to the future and path for exploitation for projects selected for funding in CBRN Cluster Part B call.

2.1.2 ENCIRCLE Dynamic Catalogue

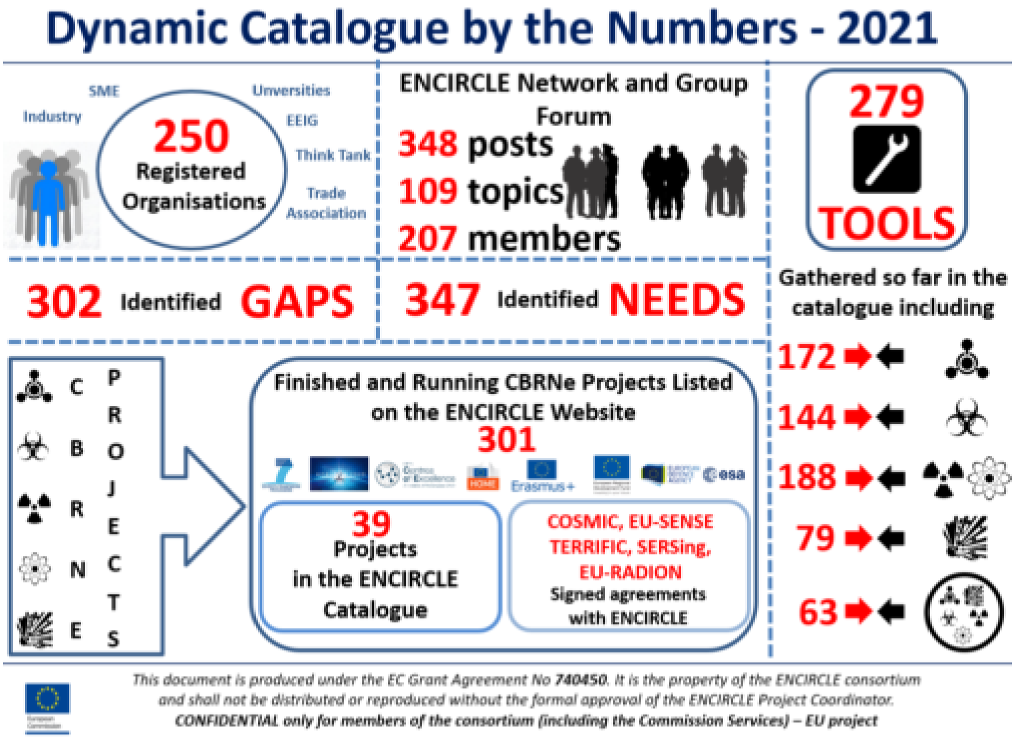
The work on further development of the catalogue has continued. Work carried out during fourth year of project realization included:

- Improvements being made to the catalogue based on user feedbacks.
- The marketplace function has been revised with the following changes:
    i. Tools List:
        - The search scope and results now include the TRL, type of CBRNe threats, keyword that are associated to the tools.
        - The results of the tools list will only include Technology Readiness Level (TRL) of 7 and above.
    ii. Projects List:

  - The search scope and results now include the type of CBRNe threats that are associated to the tools.

- In July 2020, 2 widget tools, developed by EU-VRi, were incorporated into the Innovation Watch section of the catalogue. They are the “Innovation Watch” widget, which presents potential interesting novel innovations, and the “Radar” widget that provides a pre-analysis of on-goings in the field of CBRN. In these widgets, the user can obtain the web links to the relevant articles and reports (include twitter tweets, journal reports and news articles).
- ENCIRCLE has activated a cooperation with STAIR4SECURITY (http://cen-stair4security.eu) and NO-FEAR (http://no-fearproject.eu). For this cooperation, ENCIRCLE together with NO-FEAR have shared essential metadata from their respective catalogues with Stairs4Security. The shared metadata includes information from tools, projects, needs and gaps that were collected, collated and uploaded by both ENCIRCLE and NO-FEAR community. Once the shared ENCIRCLE metadata is made available from the Stair4Security platform, discussions and reviews will continue with Stair4Security to agree on the frequency for update of this information.
- The ENCIRCLE project will officially finish on September 2021. However, the ENCIRCLE Dynamic Catalogue will still be fully operational for the next three years into 2024. And it will be maintained by Université de Nice-Sophia Antipolis (UNS)

Currently the catalogue contains.



Dynamic Catalogue by the Numbers - 2021

SME
Unversities
Industry
EEIG
Think Tank
Trade Association
250 Registered Organisations

ENCIRCLE Network and Group Forum
348 posts
109 topics
207 members

279 TOOLS
Gathered so far in the catalogue including
172
144
188
79
63

302 Identified GAPS

347 Identified NEEDS

C B R N E
PROJECTS

Finished and Running CBRNe Projects Listed on the ENCIRCLE Website
301

39 Projects in the ENCIRCLE Catalogue

COSMIC, EU-SENSE TERRIFIC, SERSing, EU-RADION
Signed agreements with ENCIRCLE

*This document is produced under the EC Grant Agreement No **740450**. It is the property of the ENCIRCLE consortium and shall not be distributed or reproduced without the formal approval of the ENCIRCLE Project Coordinator.*
CONFIDENTIAL only for members of the consortium (including the Commission Services) – EU project

Figure 1. Catalogue contents

2.1.3 ENCIRCLE Dissemination activities

The ENCIRCLE dissemination activities, coordinated by Falcon Communications, are based on the 2020 communication and dissemination plan for Period 4. All dissemination activities were actively supported by the whole consortium. The dissemination activities included:

- Sharing information about ENCIRCLE activities through use of social media, ENCIRCLE website and websites of ENCIRCLE partners.
- Disseminated stakeholder survey – June 2020
- Produced article on CBRN Challenges disseminated to the COU – June 2020
- Disseminated ENCIRCLE survey – July 2020
- Release of ENCIRCLE Magazine issue 4 – September 2020.
- Dissemination of Y4 discussions report on CORDIS for comment – October 2020.
- Dissemination of: ENCIRCLE, Human Factors PPE and COVID document - October 2020
- Promotion of the Part b call topics
- Article on ENCIRCLE in leading CBRN magazine – end of February 2021
- Release of ENCIRCLE Newsletter issue 4 – Due March 2021
- Production and release of ENCIRCLE animation – Due March 2021

Due to the challenges of COVID, ENCIRCLE was not able to participate in as many events as preceding years. We have however tried to promote the ENCIRCLE project by presenting it and also supporting other projects as much as possible in the virtual forum.

- Driver+ end of project workshop – May 2020
- EU-HYBNET meeting – May 2020
- ERNCIP-RN meeting – May 2020
- IFARI meeting – June 2020
- First responder training – June 2020
- FIRE-IN annual meeting – June 2020
- COU Meeting – September 2020
- SERSING kick off meeting – September 2020

- CEPOL 71/2020 training – October 2020

ENCIRCLE Dynamic Catalogue – Webinar

To continue engagement at a time when physical meetings were not possible, on July 7th, 2020 ENCIRCLE held the 2nd open house webinar to disseminate information about the Dynamic Catalogue. During the webinar there were demonstrations of the functionality, properties, and benefits the Dynamic Catalogue can provide, as wells as information on the latest additions and updates made to the catalogue. There was also information provided on the ENCIRCLE Innovation Watch: Radar algorithm, it's use and updates.

Part of the webinar was set aside to disseminate the results of the recent ENCIRCLE SLIDO polls results, and to hold a Q&A and discussion about the catalogue and it's use in the future. To wind up the event Philippe Quevauviller, DG HOME, ENCIRCLE Project, held a discussion about future plans and activities. This webinar was attended well and promoted discussion between attendees in the comments section during the event.

2.1.4 Innovation Watch

In order to monitor different media streams (social networks, news feeds, etc) for content from the main CBRN solution providers, main associations or clusters that may be of interest, the idea of web semantics and NSA-like methods has been further developed and customized for the CBRN topic since the beginning of the project. The dedicated user interface has been further developed since February 2019 and the BETA version of the tool. In particular, a "how to" (indicated in a menu as a "Guidance") has been developed to guide the users through the different functionalities.

The tool "RiskRadar" has been customised for the CBRN domain and is available to monitor different resource streams for content from the main solution providers, main associations or clusters that might be of interest. The tool provides the results in 2 forms: A dynamic network clustering the topics and a list of articles (with links). The Innovation Watch aka Risk Radar is available for ENCIRCLE partners testing at https://e2r2.risk-technologies.com_(username: encircle, password: encircle). Selected results are presented in the dedicated space in ENCIRCLE Dynamic Catalogue.

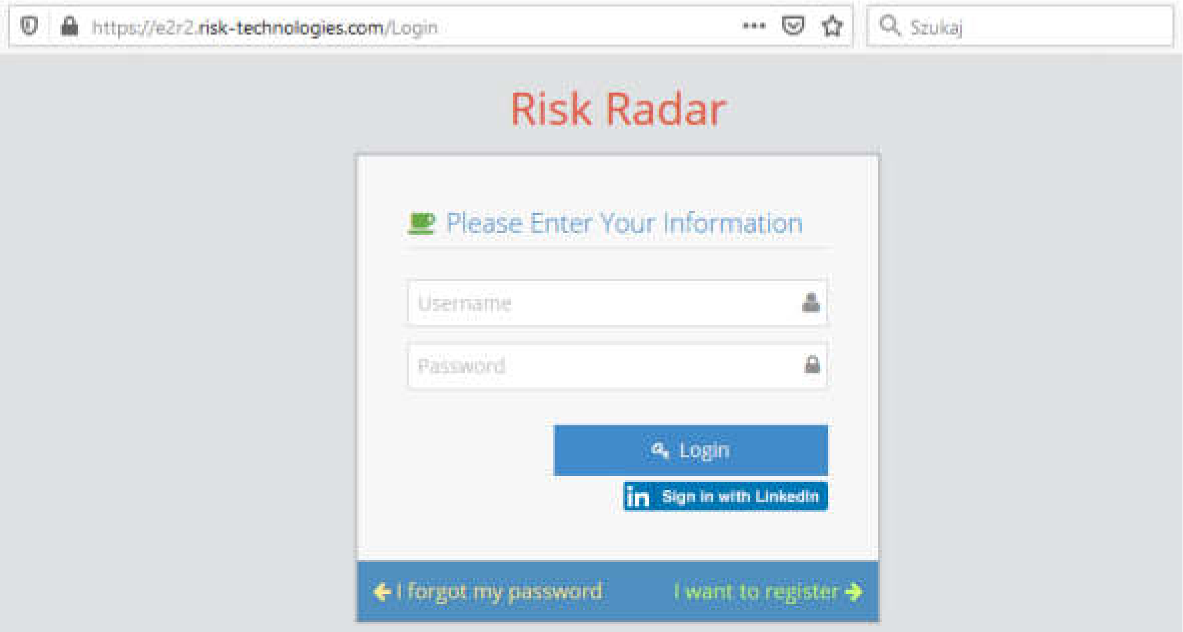


Figure 2. RiskRadar

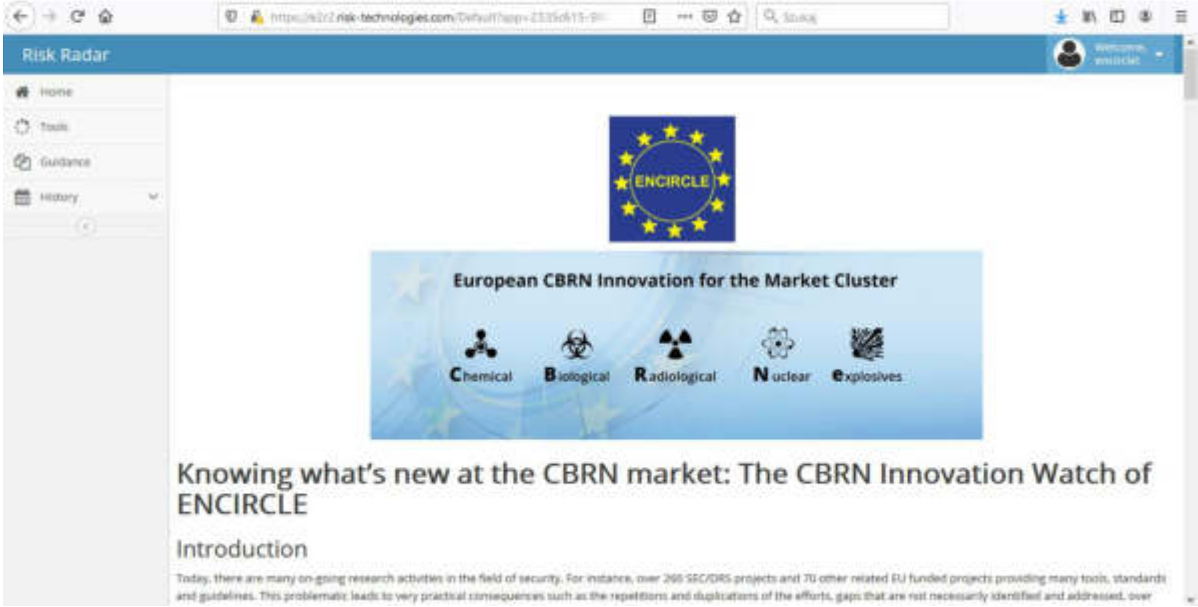
The Innovation Watch user may first read the introduction to The CBRN Innovation Watch of ENCIRCLE, which provides description of the tool and rationale behind it.

The 3-step approach of ENCIRCLE used in Innovation Watch includes:

Step 1: Identify and monitor novel online content for a certain topic

Step 2: Identify potential high impact trends - evaluating the retrieved online content to identify those texts and documents that have the highest potential for impact with using an unsupervised, quantitative big data analysis

Step 3: Visualize recommendations - providing recommendations for new innovations to be included in the ENCIRCLE catalogue by identifying those topics within the high-impact documents that have the highest novelty value



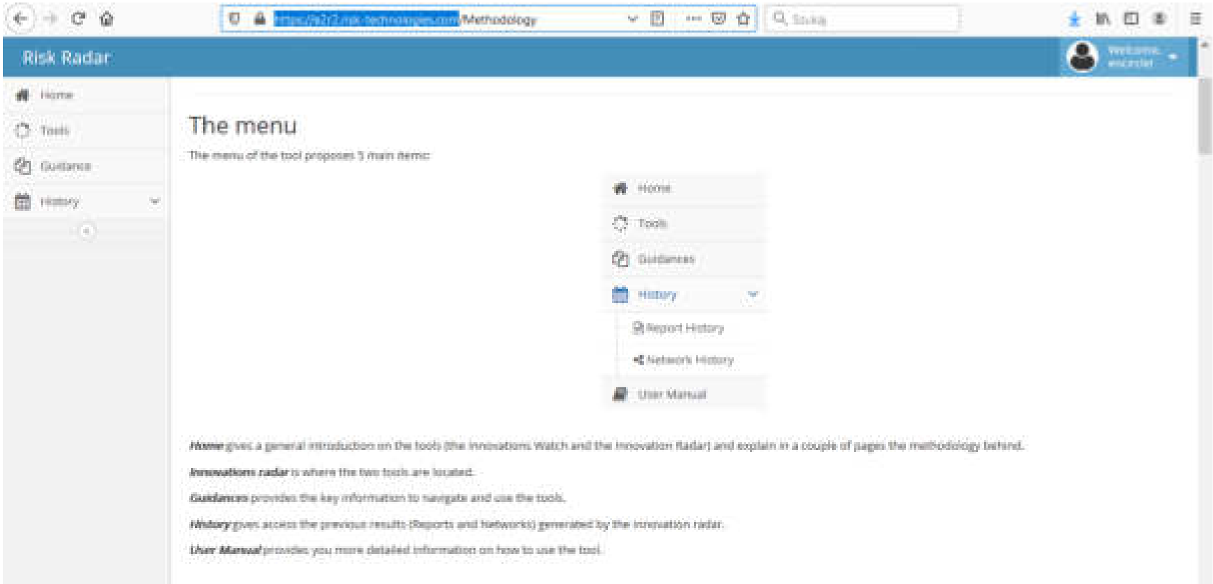
Knowing what's new at the CBRN market: The CBRN Innovation Watch of ENCIRCLE

Introduction

Today, there are many on-going research activities in the field of security. For instance, over 260 SEC/DRS projects and 70 other related EU funded projects providing many tools, standards and guidelines. This problematic leads to very practical consequences such as the repetitions and duplications of the efforts, gaps that are not necessarily identified and addressed, over

Figure 3. Encircle Catalogue

In order to make easier the use of Innovation Watch tool the "Guidance" section has been prepared and additionally the parts that were superfluous have been removed. The aim of Guidance section is to give the necessary information on how to use the innovations watch online tools to identify potential new innovations. The print screen of the part of Guidance section is shown in image below.



The menu

The menu of the tool proposes 5 main items:

Home gives a general introduction on the tools (the Innovations Watch and the Innovation Radar) and explain in a couple of pages the methodology behind.

Innovations radar is where the two tools are located.

Guidances provides the key information to navigate and use the tools.

History gives access the previous results (Reports and Networks) generated by the innovation radar.

User Manual provides you more detailed information on how to use the tool.

Figure 4. Guidance section

Finally, a five pages article dedicated the innovation watch tool has been written for the 2nd ENCIRCLE newsletter published in May 2019.

Since 2019 the tool has been made available online, so that the partners have been able to test it and provide new relevant sources to feed the tool and improve the results.

In addition, the consolidated list of sources monitored by the tool as recommended at the General Assembly has been provided. The online tool has been further developed, so that it delivers automatically the updated results in the format of the catalogue periodically (e.g.: currently every month) also used to update the catalogue. The testing and evaluation of the tool by the ENCIRCLE partners has been started, with the intention to involve all the members of ENCIRCLE communities.

2.2 ENCIRCLE COMMUNITIES

2.2.1 ENCIRCLE practitioner and technological communities.

The activities dedicated to development of ENCIRCLE practitioner's community included:

- Practitioners, are professionals that are well positioned to serve as influential members of the first responders and playing an important role in public health response to CBRN incidents. To fulfil this task, particularly during the difficult moment we have been facing and are still. We enhanced our contact with practitioners by keeping them informed about:
    - Many online workshops and web conferences
    - sharing our last published newsletters
    - Questionnaires from our part B project partners and also to
    - Questionnaires to refine the communication

- A mailing campaign to all the Practitioners and Customers community was done by both IAI and UCL, sharing the last ENCIRCLE Newsletter and inviting them to visit the Catalogue, in order to "remember" about ENCIRCLE and in line with the actions agreed during the last ENCIRCLE meeting about keeping the Community alive (June 2019)

- The Romanian PROECO CBRNe Cluster was invited by IAI to join the ENCIRCLE Community and Catalogue. IAI also invited the Romanian Cluster PoC to circulate the invitation among its network of practitioners (July 2019)

- A mailing campaign to the Italian CBRN-P3 Cluster was conducted by IAI sharing the last ENCIRCLE Newsletter and inviting to register to ENCIRCLE communities and Catalogue and to share the invitation with the potential interested stakeholders. This action was deemed useful since the Cluster is growing and there are recent new members which can be potentially interested in joining (July 2019)

- All the INCLUDING project participants were invited twice to access the ENCIRCLE Dynamic Catalogue (November 2019 and March 2020)
- Survey Launch through Network of Practitioners and also communicated to the COU 06/2020
- Invitation to participate to the Scientific International CBRN Conference (SICC) Series Web Conference « Emergency management, operative steps and actions to prepare to a new normality » (April 2020)
- Circulation of FIRE-IN project Newsletter regarding COVID-19 best practices and guidelines from European Fire and Rescue services**.** (April 2020)
- Circulation of ENCIRCLE Market Survey to Italian Cluster CBRN-P3 and RESIST project
- Invitation to participate to ENCIRCLE Dynamic Catalogue Webinar held on 7th July 2020 sent to coordinators of INCLUDING and RESIST projects (July 2020)
- invitation to **joint webinar on Just-in-time training** (methodologies, best practices in the medical, flood response and CBRN fields), co-organized by 5 EU networks of practitioners – eNOTICE, FIRE-IN, NO FEAR, DAREnet and MEDEA, the webinar is an online event, it will take place **on June 18, 2020 at 10.00-12.00 CET.**
- Distribution of Encircle Newsletter Issue4 (02/2021)
- IAI conducted a survey with the aim of gathering feedbacks from the Practitioners and Customers Community on the Dynamic Catalogue. The survey consisted in a series of questions pertaining to the Catalogue’s usefulness, ease of use, potential improvements. A written summary providing an overview of the main comments received from the Community is available (September, October and November 2020)
- Promotion to the practitioner and technological communities for e-Conference on May 18, 2021 “How could CBRNE R&I benefit from the covid-19 crisis

The activities dedicated to development of ENCIRCLE Technological and Industrial Community:

The activity concerning the technological and industrial community development during this Year 4 was oriented to direct mailing to the community members. The face-to-face meetings with industrial suppliers initially planned during professional events has been postponed in relation the pandemic situation.

- Consultation of the technological community on its approval for opening some meta data of the catalogue on public platform to enlarge tools and projects exposure. March and April 2020
- Translation and dissemination of the Slido “CBRN Stakeholder Survey” in May 2020
- Mailing to remind the Encircle market survey in June 2020 and July 2020
- Share the call for expert of TRANSTUN project in July 2020
- Dissemination of the final ENCIRCLE survey on the future development of a CBRN cluster post ENCIRCLE (02/2021)
- Industrial community information by emailing on the 4th ENCIRCLE magazine. November2020
- E mailing campaigns to encourage the Industrial community to finalize their registration process and ensure optimal identification of their tools for an effective communication with the future CBRN cluster.
- Mailing in February 2021 to catalogue companies to participate to the virtual exhibition space during the CoU CBRN State of the Art conference on May 2021.

2.3 MARKET AND BUSINESS SUPPORT

2.3.1 Market analysis

Building upon the 2018 Market Analysis Report, a number of polls have been conducted primarily using the SLIDO platform. These polls were available in the English, French, Italian and German languages and were targeted at the industrial and practitioner and technological communities.

As was the case with the polling conducted for the 2018 poll, the number of responses garnered for these latest polls were not as widespread as would have been ideal and the ability to be able to get a large response clearly remains an issue going forward. The reasons for the difficulty in being able to achieve a large uptake can only be speculated at but undoubtedly the scarcity of first responder practitioner time to participate in such exercises – especially against the COVID-19 background – must be a key and relatively constant factor. It should be noted that there was a conscious decision to keep a core of the most recent polling questions substantially either the same or closely related to the questions used in the 2018 poll in order to try and better identify any linear trends. A separate joint market analysis exercise was also conducted with the TERRIFFIC project.

The results of this latest polling have been made available in an updated ENCIRCLE market analysis report which will be accessible via the ENCIRCLE Networks & Groups Forum, under Resources. A high-level summary of some of the findings are as follows:

- Many of the attitudes toward the market identified in the 2018 Market Analysis Report remain valid, including, for example, the slightly anachronistic attitude towards Standards where similar numbers of respondents identified that they believed Standards to be helpful in terms of encouraging innovation and new market entrants but these were 'balanced-off' be the number of respondents who thought that the Standards applicable to CBRN were outdated and of little use. A similarly consistent theme emerged with respect to the perceived importance given to the need for PPE (and improvements thereto) and the need for better CBRN Information Management/Situational Awareness systems (or, "Warning & Reporting" in NATO military language), particularly for systems that could be used for civilian response, which in turn both creates and sharpens the implications around the need for better interoperability, both between military and civilian response and amongst the different civilian response organisations; this of course then raises further implications in such areas as Standardisation, Communication Protocols/Interfaces and terminology. The area of Detection, Identification & Monitoring (DIM) was also a consistent area where technological improvements are perceived to be needed;
- It was not entirely clear at what point per respondent the effects of the COVID-19 situation manifested themselves and to what degree of depth (the 2020 Poll closed 31.7.2020, but many of the responses were received well prior to this date) , suffice to say that a clear consequence was that biologically based threats had significantly moved up from the 2018 survey rankings and were now seen, along with the 'new' category of "hybrid" threats introduced for the first time in the 2020 poll, as the major threat source in the coming 5 – 10 year period. In the coming 12 -24 months it will be interesting to see what the longer term consequences of COVID-19 will be: it may be that the financial consequences of the widespread lockdowns to individual national economies will be bound to result in less funding being available than might normally have been expected, and/or; as happened with Ebola in 2014, it may that there has been a 'disconnect' in the minds of people within governments of a pandemic with CBRN (when, in fact, many of the containment and response lessons were already well known to CBRN professionals as part of 'normal' CBRN disciplines). Suffice to say that in a post COVID -19 world many of the survey responses and views which ENCIRCLE (and others) have garnered over the last two years might well be changed with consequent impacts on the market and technology supply base which might be difficult or impossible to predict currently.

2.3.2 Business Models and Plans and Financial Instruments

A list of financial instruments has been included on the ENCIRCLE project website[1] and in the forum. However, the European Commission site already provides this function[2] and the project has been directing projects to this site rather than duplicate effort.

In addition, there is an opportunity for small and medium size companies via the new EIC accelerator which was previously the SME instrument. The main focus of the EIC accelerator[3] is on market-creating innovations.

During the last year the business maturity model has been developed further and used to baseline and monitor TERRIFFIC, EU-SENSE and COSMIC and virtual meetings have been held to baseline the two new projects EU-RADION and SERSING. The purpose of the model is to identify the gaps that will need development to improve the business success of the projects. Initial discussions on plans for exploitation have also been conducted although most of the areas support required from the projects has been around dissemination and awareness and standards. ENCIRCLE and TERRIFFIC have also jointly collaborated on a market analysis study.

On the standards area, ENCIRCLE is actively collaborating with Stair4Security and a pilot exercise is being conducted to provide a copy of some of the elements of the ENCIRCLE platform onto the Stair4Security platform.

2.4 INTEGRATION AND TECHNICAL SUPPORT

2.4.1 Standards and Interfaces

During the reporting period, there was further development of the standards and interfaces database through consultation with the practitioner network projects – NO-FEAR, INCLUDING and FIRE-IN and from the results of the ENCIRCLE surveys. In addition, collaboration has been made in this period with the Stair4Security project concerning standards development. A final standards and interfaces databases is available as an ENCIRCLE resource and has been shared with the other projects. ENCIRCLE has also noted the references to standards in the recently published EU action plan on synergies between civil, defence and space industries and in particular ACTION 5: “Before the end of 2022, the Commission, in close cooperation with other key stakeholders, will present a plan to promote the use of existing hybrid civil/defence

[1] http://encircle-cbrn.eu/resources/funding-instruments/

[2] https://europa.eu/youreurope/business/finance-funding/getting-funding/access-finance/index_en.htm

[3] https://ec.europa.eu/easme/en/section/sme-instrument/eic-accelerator-funding-opportunities

standards and the development of new ones." The ENCIRCLE list of standards already contains civil and defence (NATO) standards

2.4.2 Integration Platforms

During the reporting period, Miksei continued supporting ENCIRCLE surveys and workshops conducted concerning integration issues around standardization, interfaces, and civil protection symbology. Meanwhile cooperation and commenting with other tasks and collaboration between Part B projects have continued. That was done via promoting data interchange between part B projects and other European CBRNE communities. Also, more Finnish NCPs are informed about Encircle project and its results. Miksei has been organizing and finalizing this D5.4 Impact Report Y4 too.

2.4.3 Impact Policy and Exploitation

The impact of the developments of the ENCIRCLE consortium has been measured in several ways – they are presented in a report that is not a public deliverable, and whose front cover being the annex to this Deliverable (ENCIRCLE Cluster Impact Y4 Annex 2 Results of the ENCIRCLE's developments impact analysis). The first measurement was focused on the impact of consortium's dissemination activities on the number of registrations in the ENCIRCLE's online catalogue and forum, containing solutions for counter-CBRNE response and a networking space, as well as on introducing new and updating existing entries in the catalogue. According to the analysis, there is a slight correlation, despite the nature of the activity (newsletter/conference/webinar/etc.). In some cases – where the activity was focused on promoting the online solutions, the correlation is more visible. Other types of the activities didn't help in attracting so many new users to the catalogue or encouraged them to upload/update more information. A resulting guideline could be the organisation of the dissemination events focused on the particular aspect of the project – like the announcement of the webinar on the catalogue pulled many users before the event. As the analysis was planned during the second half of the project, there is no available data on the details of the dissemination activities such as number of handed out project flyers or business cards that may be supportive to more detailed analysis. In case of any future project willing to measure its impact in the end the consortium partners should consider starting the analysis at the beginning of the project. This would allow to gather data starting from the early phase of the project which will provide more useful and valuable information in the broader context. The ENCIRCLE's impact analysis also included only dissemination activities reported in Work package 3, so there are no results coming from other/minor activities, such as personal meetings or activities carried out during events of other projects and initiatives.

The second measurement of the impact was focused on the analysis of the usage of the catalogue and forum by the users. This analysis operated on raw data from the server logs, which were not designed to provide detailed data at the beginning. The most important message that is provided in the analysis is the fact, that many potential users, which abandoned the registration process, are marked with "halfway" status, which does not allow them to access the online services. This may be caused by various reasons, but some cases can be explained by the complex process of the registration, which, in the first version, required a support letter from the employer. The other possible reason may be that the registration has to be approved by ENCIRCLE's representatives, so in case of the delay in approval potential user could lost interest in logging. The lesson from this is to provide the registration process as easy as possible, with respect to security issues - as the catalogue provides detailed information about the special products and direct contact details to the producers, it shall be protected from inappropriate use.

In order to make the entry point for new technical suppliers easier, the analysis of the documents from European level and from selected Member State on security and defence procurement has been prepared. It is available in the form of report being an annex to this Deliverable (ENCIRCLE Cluster Impact Y4 Annex 1 - Results of the analysis of the legal documents concerning security and defence procurement).

The report contains the list of the most important, difficult, and tricky obligations, that must be fulfilled by the suppliers and points some areas, that could be changed to make a more supplier-friendly environment. The analysis has shown that suppliers of security and defence agencies are burdened with various organisational requirements, that have been introduced e.g., to provide safety for the whole chain of delivery of products as well as the producers, their facilities and end-users. Due to the fact, that special products can be used also by unauthorized people or criminals/terrorists, great focus is set over the production, storage, transfer and trading processes. This generates additional requirements to be fulfilled.

Although there are only a few European level documents that provide details on these processes, the necessity to implement them into national law (transposition) and possibility to introduce additional rules by Member States has resulted in a high number of documents, with whom the supplier of special products needs to understand. For example, in Poland there is a number of documents that presents rules of conducting business activities (some of them are mentioned in the one of WP5 reports), but there are an additional number of documents with more rules that needs to be analysed by the supplier to have a full picture of obligations. The situation is even more complex in case of procurement carried out by the Ministry of Defence, which has got its own documents, and are further adjusted in the way to protect the essential security of the State. Thus, the supplier has to assess a large amount of documents in order to fully understand the process and not omit or simplify too much something that is important, as there may be penalties. The variety of documents also contains many references to other ones (and required considerable effort for this analysis). This creates an environment where it is easy to forget something important and where the entry point is sometimes hidden behind huge organisational and financial investments, which need to be covered by the suppliers.

The main conclusion coming from this analysis is the necessity of creation of some kind of manual or at least a list of the security and defence documents at the governmental level (and by governmental agency). Whilst the general instructions for the conducting business are available they still don't contain all the information and there is a lack of instructions for security and defence procurement. Such a compilation would help introduce the rules to new suppliers, and in particular for SME's, decreasing the probability of making a big mistake. Another problem that should be solved is the need to monitor the changes that are being introduced to particular documents by legal processes. Such updates often reference or even change additional documents related to the topic. Due to the fact that security and defence procurement requires knowledge of such a high number of documents, tracking of their changes is very hard and the supplier need to monitor consistently for any changes. If there was a complied information on the topic (e.g. mentioned earlier list of documents or a manual) it would be easier and faster to find necessary information.

2.4.4 Human Factors

On 13.03.2020 the head of World Health Organization (WHO) reported that Europe was becoming the new epicentre of the COVID-19 pandemic and as Task we felt the need to give our contribution to the discussion. The non-deliverable document was designed to discuss some of the considerations that were already made by different entities (i.e. Royal College of Nursing) and to organize them in a useful way for stakeholders. We considered PPE availability, problems associated with PPE, badly fitting PPE and the procedures that the Healthcare workers are asked to perform while dressing PPE as well as other factors implicated. The document has not the objective to be exhaustive and comprehensive since the COVID-19 pandemic is still ongoing and we expect many contributions on this. To conclude, the scope of the PPE is to provide protection but, thanks to new materials and know-how, we might expect an improvement of ergonomics, helping HCWs (Health Care workers) to carry out their activities in an easier way. The process of PPE re-design should more involve all the actors, from end-users to manufacturers, taking into account the users' needs and new technologies.

Thanks to the invitation received together with many other H2020 projects for contributing to European COVID-19 Data Platform[4] the authors, together with the coordinators decided to make the research on Human Factors associated with PPE for Healthcare workers freely available on the ENCIRCLE website; Moreover, a short summary of the conclusions was included in the Issue 4 of the ENCIRCLE Magazine. The analysis of the Human Factor questionnaire, produced in 2019, is available only on the portal.

2.5 FEEDBACK ON PART B RESEARCH AND DEVELOPMENT ACTIVITIES

2.5.1 TERRIFFIC

The first hours of response to a CBRNe incident, and especially a radiological event, are particularly critical to contain the most severe consequences, stop the ongoing criminal or terrorist threat, save victims, manage the crime scene and organise an effective response by all concerned stakeholders – firefighters, health responders, forensics, police, decontamination units. They are also the riskiest moments for the first and second responders, as the nature, extent and intensity of the contamination is still unknown and other booby traps and contaminated objects may still be present.

The solutions provided by the TERRIFFIC project are tailored to the needs of practitioners and will allow for less human intervention in the operation, due to a higher number of automated processes and improved and extended mobile detection capabilities in the 'hot zone'.

Improved situational awareness and the delivery of near real-time data within the TERRIFFIC System will result in a better Common Operational Picture. This will enable incident commanders to gain a better comprehension of the nature and scope of the threats and therefore make better-informed decisions.

[4] https://www.covid19dataportal.org/

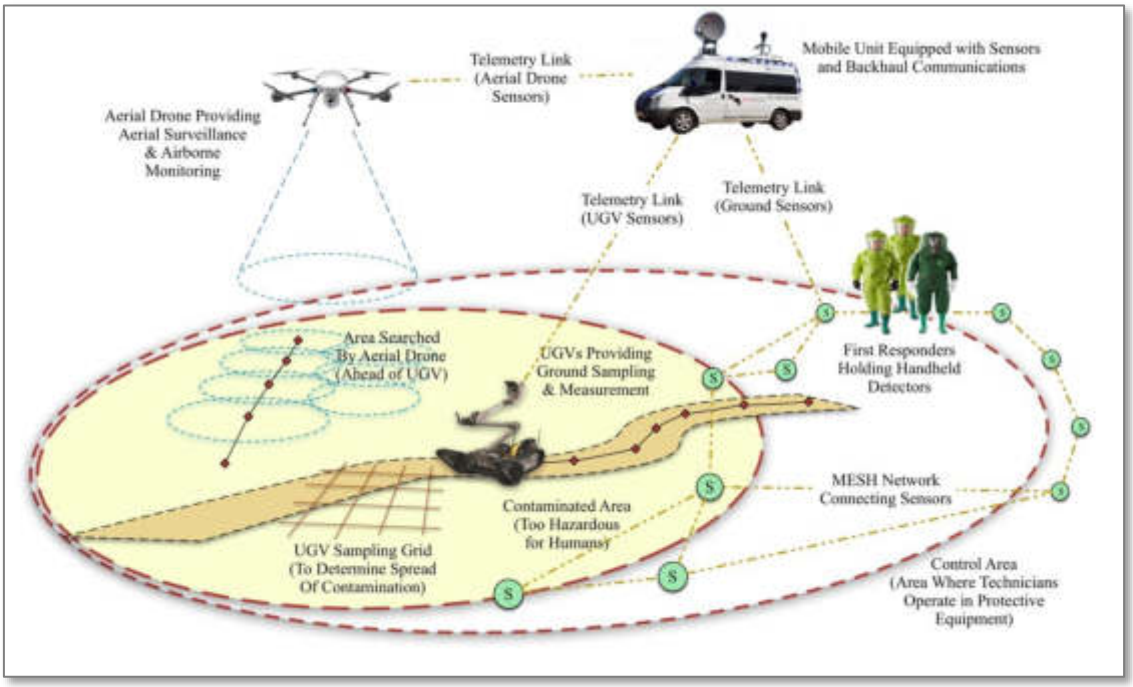

Aerial Drone Providing Aerial Surveillance & Airborne Monitoring
Telemetry Link (Aerial Drone Sensors)
Mobile Unit Equipped with Sensors and Backhaul Communications
Telemetry Link (UGV Sensors)
Telemetry Link (Ground Sensors)
Area Searched By Aerial Drone (Ahead of UGV)
UGVs Providing Ground Sampling & Measurement
First Responders Holding Handheld Detectors
MESH Network Connecting Sensors
Contaminated Area (Too Hazardous for Humans)
UGV Sampling Grid (To Determine Spread Of Contamination)
Control Area (Area Where Technicians Operate in Protective Equipment)
S

Figure 5 TERRIFFIC Concept of Operations (SOURCE TERRIFFIC)

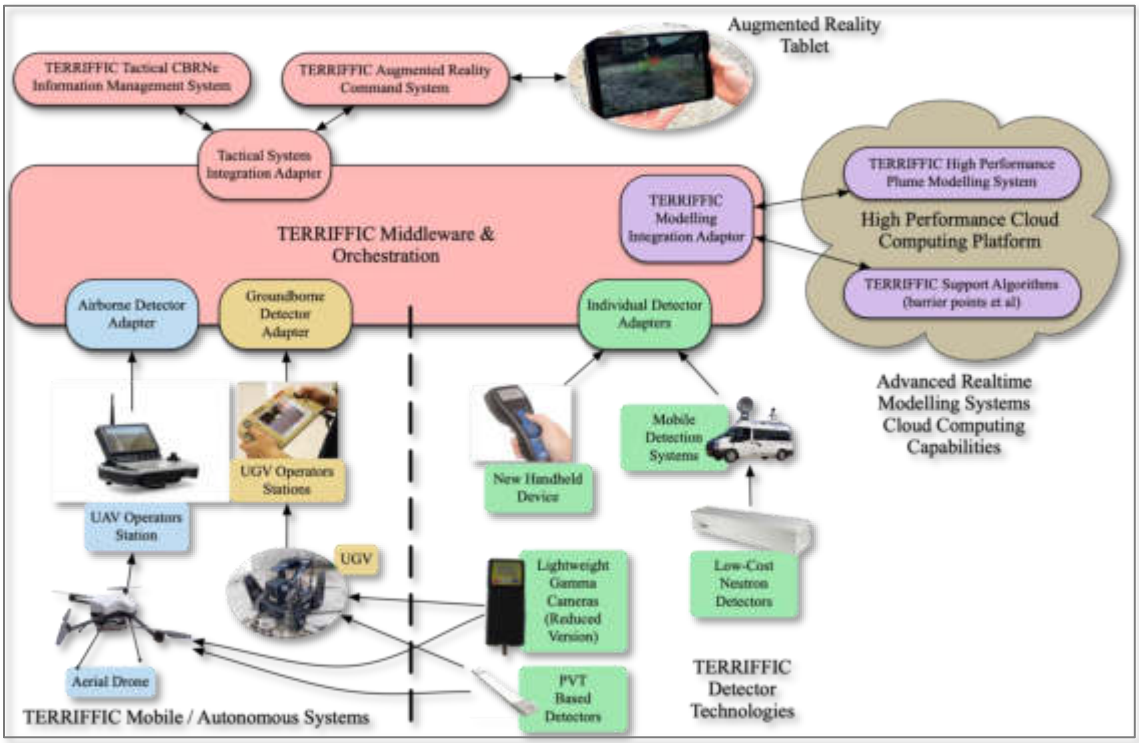

TERRIFFIC Tactical CBRNe Information Management System
TERRIFFIC Augmented Reality Command System
Augmented Reality Tablet
Tactical System Integration Adapter
TERRIFFIC Middleware & Orchestration
TERRIFFIC Modelling Integration Adaptor
TERRIFFIC High Performance Plume Modelling System
High Performance Cloud Computing Platform
TERRIFFIC Support Algorithms (barrier points et al)
Advanced Realtime Modelling Systems Cloud Computing Capabilities
Airborne Detector Adapter
Groundborne Detector Adapter
Individual Detector Adapters
UAV Operators Station
UGV Operators Stations
UGV
New Handheld Device
Mobile Detection Systems
Lightweight Gamma Cameras (Reduced Version)
Low-Cost Neutron Detectors
PVT Based Detectors
Aerial Drone
TERRIFFIC Mobile / Autonomous Systems
TERRIFFIC Detector Technologies

Figure 6 TERRIFFIC Architecture (SOURCE TERRIFFIC)

2.5.1.1 Objectives of the TERRIFFIC Project

Objective 1 Deepen the shared understanding between practitioners and (technological) solution providers on the needs/requirements during the "first hours" of response and technological possibilities and features matching them

Objective 2 Create the open architecture of the TERRIFFIC System, which promotes (future) integration of (existing) solutions and develop an innovative user interface enabling practitioners to easily deploy the system during immediate response

Objective 3 Adapt promising existing solutions from previous research initiatives, convert them into TERRIFFIC core components and integrate them into the TERRIFFIC System

Objective 4 Develop novel solutions on mobile sensing, measurement devices and dispersion models and integrate them as core components into the TERRIFFIC System

Objective 5 Successfully test the TERRIFFIC System and its core components under demanding lab conditions and within field trials to demonstrate the reduction of response time within the "first hours" of a RNe incident

We can report that Objectives 1, 2, 3 and 4 have been achieved and significant progress has been made on Objective 5, the only limiting factor being the impact of the travel and meeting restrictions caused by the national Covid-19 lockdowns. These have meant that although a face-to-face integration meeting was held at Arktis Radiation Detectors' premises in Zurich on 07-09 September 2020, a final physical integration meeting, scheduled for November, had to be postponed.

Once this (post-lockdown) integration and testing meeting has been held, then we will be able to test the TERRIFFIC System with practitioners both in a tabletop exercise in Slovakia and operationally in the Final Trial in France. Dates for these events will be scheduled as soon as the respective governments have confirmed the timing for the easing of lockdown in each country.

The delays caused by the Covid-19 restrictions have meant that we are in the process of submitting a request to the Project Officer for a six month extension to the project to allow us to complete all the tasks and requirements of the Description of Action. If approved the project will run until the end of October 2021.

2.5.1.2 Updates from Technical Partners

Bruhn NewTech

- Development of established incident management software that can accept and share data from various external tools and solutions, including detectors, sensors, cameras, plume modelling and mixed reality, providing improved situational awareness in a user-friendly format

- Plan to extend mapping engine to support 3D visualisation and the latest NATO standard for Warning and Reporting.

École Centrale de Lyon

- Sensor that detects the location, type and size of a radiation source and plume modelling
- Development of the plume software which aims to characterise the RNe source (position, release rate, nuclide type) and estimate the associated safety zone. This software is composed of two complementary main building blocks: a direct model and an inverse model.
- The direct model, composed of an atmospheric dispersion model called SLAM (Safety Lagrangian Atmospheric Model) and a gamma radiation model named MARIE (Model for Atmospheric Radiation Indoor & in Environment), allow the user to estimate and forecast the fluence/dose rate field, induced by an RNe source(s) in a complicated urban environment. Conversely, the inverse model, called ReWind, aims to characterise a RNe source based on fluence/dose rates measured by sensors.

Luxembourg Institute of Science and Technology

- Development of an augmented reality system that displays cordons and real-time information from UAVs, UGVs and hand-held sensors. It also supports annotations and what is displayed can be adapted depending on the role or security level of the user.

The French Alternative Energies and Atomic Energy Commission (CEA)

- Development of the world’s smallest Nanopix gamma camera in its advanced version that weighs around 300g, which is important so it can be mounted onto light UAVs / UGVs and includes automation capabilities and close-to-sensor intelligence.
- New hand-held beta contamination probe that allows beta contamination to be detected in a high and fluctuating gamma background without interferences. Enhanced electronics are able to provide GNSS location information and connect to a wireless infrastructure for mapping of contamination levels.

AERACCESS

- Adaption of the Hawker Q800X, a ruggedised UAV, which can fly in higher winds (70kph with gusts up to 90kph), rain and other adverse weather conditions, to take the Nanopix gamma camera and the high sensitivity SiPR gamma detector as additional payloads and feed data back into the incident management system; successfully used in trials integrated with Bruhn NewTech incident management system and École Centrale de Lyon plume modelling software,
- Smaller NanoHawk UAV flown in tests inside a building with a camera and located a radiation source; larger drone used to relay communications to Nerva XX UGV and extend its mission range

Nexter Robotics

- Adaption of the Nerva XX UGV to take the Gamma camera and Gamma detector, providing more accurate data and imagery from inside the hot zone

ARKTIS Radiation Detectors

- Successful integration of the TERRIFFIC System inside the MODES mobile detector van
- High sensitivity SiPR Gamma detector developed and tested on UAV and UGV

2.5.1.3 Benefits of the Project – a step-change in first responder efficiency

The TERRIFFIC System consists of a set of complementary, interconnected and modular software and hardware components, which represent both novel developments of innovative technologies as well as enhancements and optimisations of existing solutions.

The TERRIFFIC System and its core components are highly mobile and will be able to be deployed quickly. The tactical incident management system installed on the mobile van will be initiated whilst en route. The van will also be equipped with easy to set up ground detectors for immediate deployment on-site, as well as having handheld detectors for use once the initial assessment of the risks has been completed.

Specialist UAVs, able to fly in rain and gusts of up to 90kph, with the world's smallest gamma cameras and new sensors attached, can be operational within minutes and will be used to visualise and identify the location, size and type of the source. They will also be able to spot potential victims and communicate visual data about damage and people needing assistance.

UGVs with sensors and cameras can be sent in to obtain further data from closer up. The data that these sensors provide are used to create a plume modelling forecast, which will give a more accurate and dynamically updated determination of the contaminated area and the control area. The plume modelling algorithms have been specifically designed for use in complicated urban environments and take into account the wind, weather and surrounding buildings, which will all affect the radiation dispersal.

All of these tools send information to the augmented reality solution and the incident management software concurrently. This greater knowledge results in a reduced risk profile and a higher level of safety for first responders.

It has never before been possible for a CBRNe incident commander to be able to access so much data in near real-time. The TERRIFFIC System has the potential to have a significant and genuine impact on how an RNe incident is managed by first responders and more importantly to save lives both of practitioners and members of the public.

2.5.1.4 Main Dissemination and Exploitation Achievements

Frost & Sullivan was commissioned to prepare a market analysis report of the CBRNe market, as part of the work in Task 7.6 – leading to the completed deliverable *D7.4 Exploitation*

Strategy and Business Plans. Entitled **Growth Opportunities of Emerging Technologies Impacting CBRNE Applications - Sensors, Drones, Robotics, and Wearables Drive Opportunities in the CBRNE Industry**, this initiative was jointly funded with ENCIRCLE and the report has been shared with both consortia's partners. Whilst it did provide some useful and informative qualitative data for us, it did not include any in-depth financial insights into the value and volume potential in the market for the SME partners. To provide this additional in-depth analysis would have been financially restrictive and not felt to be a valuable use of budget.

Three of the consortium partners have so far signed contracts and are already working to exploit their components jointly to their existing and prospective customers, both during and after the project. Very positive discussions are moving forward in particular with Armasuisse, which has expressed interest in the general project and for certain specific components – drone detector assemblies and the gamma camera. Other partners are also in discussion regarding the opportunities to exploit the project's Results, although they have not yet signed formal contracts.

The planned Semi-Public Workshop was held virtually on 11th December with over 40 CBRNe practitioners, experts, consortium members and representatives from other research projects participating in this one day online event. Consortium partners reported on the current progress of each element of the project and the feedback received after the Workshop has all been very positive. Several options had previously been explored for a physical meeting, with meeting rooms reserved in hotels, but the Covid-19 restrictions made this option unfeasible.

A social media communications campaign was run from September to December on both LinkedIn and Twitter, which received 28,806 views and 17,723 impressions respectively. This covered the integration and testing week and the build-up to the Semi-Public Workshop. This campaign disseminated the Results and also raised awareness about the project's overall work to a wider CBRNe audience. We now have built up a community of 829 CBRNe professionals on LinkedIn, to whom we will continue to disseminate the work and inform them about the results of the field exercise, Final Trial and the final Public Workshop.

Two articles will shortly be published in the International Firefighter and NCT magazines, both leading specialist media. A press release is being distributed to all contacts in the specialist media during week commencing 22 February. The focus in both the release and the IFF article is on the potential benefits of the TERRIFFIC System to critical national infrastructure operators, agencies and organisations.

2.5.1.5 Contact Information

If you would like to know more about the TERRIFFIC project, please visit the project website at www.terriffic.eu or contact us by email:

Project Coordinator – Ulisse Gendotti, ARKTIS Radiation Detectors

gendotti@arktis-detectors.com

Project Communication and Media Contact – Rob Munro, ARTTIC terriffic-arttic@eurtd.com

2.5.2 EU-SENSE

Chemical Agents have been used in warfare against military personnel for almost two centuries, however, with increased terrorist activity in recent decades, the scope of defence effort has broadened to include the more significant threat posed to civilians. Both military and civil defence require fast and reliable methods for detecting agents at levels that pose a health risk for accurate assessment of severity and extent of hazard and efficient use of countermeasures. Civic defence resources, in addition, face the threat of industrial incidents resulting in dangerous contamination of environment.

The consortium composing the EU-SENSE project took on developing a novel network of sensors capable of detecting a large spectrum of chemical agents. The objectives of the project are primarily:

- To contribute to better situational awareness of the CBRNe practitioners through the development of a novel network of chemical sensors, which will provide a technological solution to relevant gaps presented in the ENCIRCLE catalogue of technologies
- To improve the detection capabilities of the novel network of chemical sensors through the use of machine learning algorithms to reduce the impact of environmental noise and the application of contaminant dispersion models
- To showcase the usability of the EU-SENSE network to CBRNe practitioners in order to validate the system and to maximize its exploitation potential. The objective also entails the preparation of training sessions with CBRNe practitioners in relevant conditions.

The technical concept of the project is based on three layers. The first - the network layer - consists of heterogeneous sensor nodes that combine detecting capabilities of four different detectors, including Proengin AP4C (Flame Photometric Detector), Airsense GDA-P (Gas Detector Array – Personal) detector (IMS with Electrochemical Cell), Airsense GDA-P detector (IMS with Photon Ionisation Detector, and TNO Metal Oxide detector. Additionally, each node has an integrated GPS module for node positioning purposes. Those sensors are integrated through the Network of Sensors Controller and visualised in Situational Awareness Tool

The second - computational layer - is constructed in compliance with the system-of-system approach through the use of independent tools:

- Source Location Estimation Tool – runs a dispersion engine to assess location and strength of the hazard's source
- Hazard Prediction Tool – performs dispersion calculation to predict the behaviour of the incident
- Environmental Noise Learning Tool – utilizes machine learning to minimize the false alarm rate.

The final layer is the situational awareness layer consisting of the main user access point to the - the Situational Awareness Tool, with the graphical interface that renders visualisation and control functionalities – as well as integrated training module.

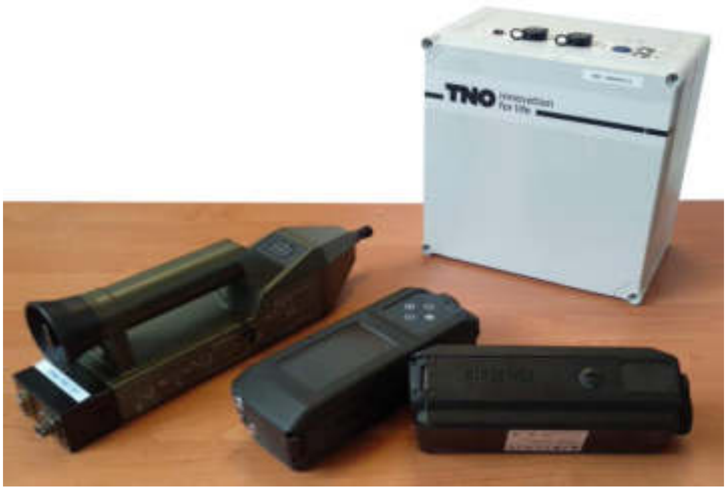
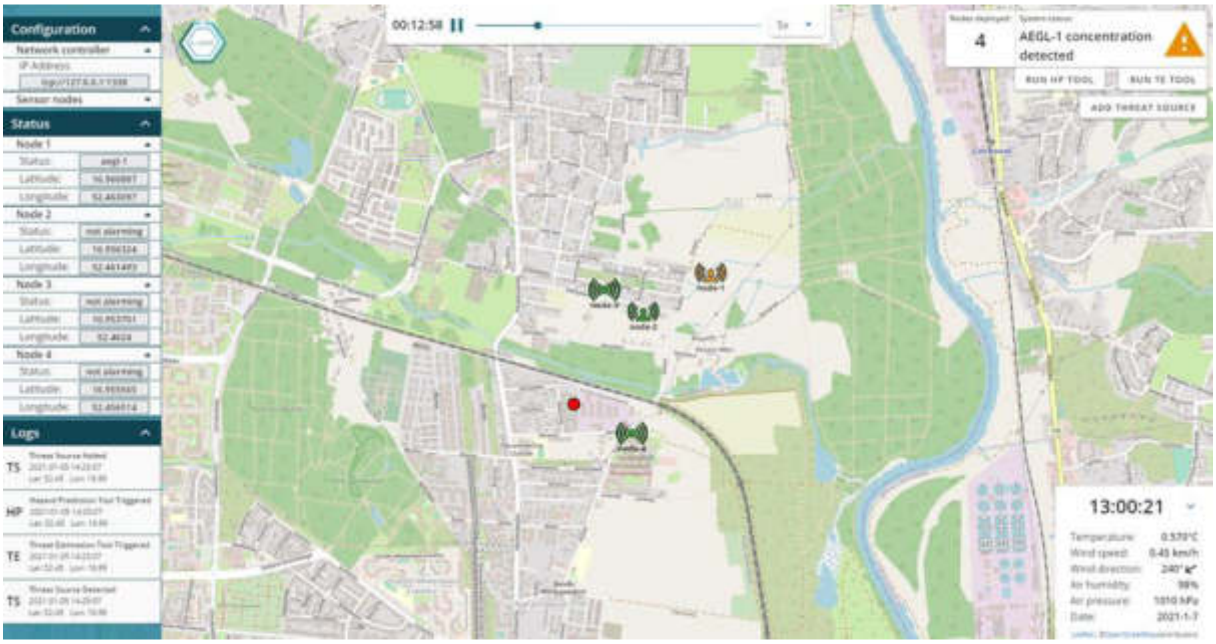


Figure 7. The four sensors of the EU-SENSE sensor node. Source: EU-SENSE

The project is currently in advanced stage of development. The recent months concluded work on the third (and final) generation of the sensor node. The hardware prototype was also tested in a measurement session that relied on exposing the integrated nodes to simulants such as Ammonia and TEP (triethyl phosphate). The design and development are progressing for the Hazard Prediction Tool and the Source Location Estimation Tool, as well as Situational Awareness Tool. The consortium partners are currently working on improving the computational tools and integrating them with the developing Graphical User Interface (GUI).



IP Address: [illegible]

Node 1
Status: aegl-1
Latitude: [illegible]
Longitude: [illegible]

Node 2
Status: not alarming
Latitude: [illegible]
Longitude: [illegible]

Node 3
Status: not alarming
Latitude: [illegible]
Longitude: [illegible]

Node 4
Status: not alarming
Latitude: [illegible]
Longitude: [illegible]

TS Threat Source Added [illegible]
HP Hazard Prediction Tool Triggered [illegible]
TE Threat Estimation Tool Triggered [illegible]
TS Threat Source Detected [illegible]

00:12:58

Nodes deployed: 4
System status: AEGL-1 concentration detected

13:00:21
Temperature: 0.570°C
Wind speed: 0.45 km/h
Wind direction: 240°
Air humidity: 98%
Air pressure: 1010 hPa
Date: 2021-1-7

Figure 8. The EU-SENSE Graphic User Interface (in development)

Despite the immediate impact of the pandemic outbreak on the project, there was a significant impact on progress on the dissemination efforts within the project. The main affected area was the field measurements necessary for the machine learning progress in the Environmental Noise Learning Tool. The planned conferences and publications, however, were made possible through the effort of their respective organisations, like the International Society for Optics and Photonics, organisers of SPIE Defence + Commercial Sensing, where ITTI presented the project, as well as published extensive paper on the systems architecture and ambition.

If you would like to know more about the EU-SENSE project, please visit the project website at https://eu-sense.eu/.

2.5.3 COSMIC

2.5.3.1 Objectives and concept of the project COSMIC

Modern customs deal daily with tenths of thousands of containers, potentially containing CBRN threats. They currently open some containers for inspecting them, sometimes basing on the manifest of the cargo and some additional knowledge from the custom administrations. H2020 Profile project[5] is currently working on the automatic analysis and incorporation of data from different sources, resulting in an improved selection of the containers to inspect.

[5] https://www.profile-project.eu/

But even with this automatic profiling of the cargos there are still several challenges to face:

- Manual inspection of the containers remains very expensive in terms of both of devoted resources and consumed time
- Smugglers and terrorist may still succeed in hiding their threating content in the cargo

Hence, it is necessary to equip the custom offices with technologies to detect the threats more effectively and an inspection mechanism that is much more cost effective than the current one. Accordingly, COSMIC consortium has rethought from scratch the whole operation in customs and proposes the following process of containers in the customs as a three phases procedure:

- At any time, the custom operator may decide to take any container directly for manual inspection;
- In a first phase, custom operators will run a first screening of each container with low-cost sensors with average precision and fast response times to detect if there is any potential threat of the main types (explosive, chemical and radiological). From this, the many containers that do not trigger any alarm are released with very little cost;
- In a second phase, containers that triggered an alarm proceed to a second row (letting the rest of containers to continue its process) and are screened with more accurate sensors, at the cost of being more expensive and taking more time to perform their calculus, but as they are applied only to the second row, they will not cause any significant delay in the processing of the whole processing chain. If the sensors of the second phase detect any threat, the container proceeds to the third phase for manual inspection; and
- In a manual inspection phase, the containers will be opened to physically locate and isolate the threat, and to further clarify the nature of the threat in the case of biological threats.

However, detecting threats from sensors still have the following challenges:

- X-ray is limited in its capabilities
- Radiation detection results of RN threat material is matrix dependent
- Shielding / masking is seen across the organic-inorganic-metal material spectrum

Additionally, there is no 100% accurate sensor, especially because the attackers will do their best to hide the threatening materials from them. Thus, sensors normally produce detection probabilities, using probability thresholds for triggering the alarms. Besides collecting the measures taken from the sensors in each phase, COSMIC combines those measures with the manifests to execute automatically the profiling that was performed manually by the customs authorities, refining the probability obtained from sensors while still using the knowledge of the customs authorities.

This optimized process requires a graphical tool to let customs operators follow the whole process and assess the risk for each container. COSMIC has developed an advanced and user-friendly graphical tool that allows customs operators to easily follow the progress of each container, its measurements, possible threats detected and evolution through the process.

2.5.3.2 Progress up to date

2.5.3.2.1 Data sensing capabilities

Explosives detection

An explosive vapour detector has been developed which includes the capability to be considered both as primary inspection and secondary inspection system depending on the internal configuration of the system. The proposed detector relies on the DMA-MS (Differential Mobility Analyzer – Mass Spectrometer) technology as it can be seen in the following picture. Vapours retained in the filter are inserted in the thermal desorber where they are liberated, and subsequently ionized in the SESI ionization source. After that, ions are filtered in the DMA by their electrical mobility and then, in the MS by their molecular mass.

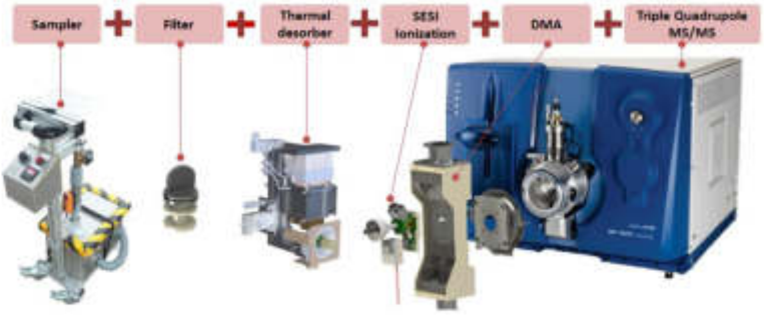


Figure 9. Explosive vapour detector. SOURCE COSMIC

The primary inspection system offers a high throughput capacity (one analysis per minute) at the expense of a little reduction in the detection capabilities (detection rate and false alarm). This elevated level of inspection is achieved thanks to the fast mobility tuning in the DMA. On the other hand, the secondary inspection system has a very high detection rate (0.01 ppqs) and very low false alarm ratio (<1%), but the required analysis time is in the order of some minutes since a more precise mobility analysis is required, which includes the analysis of the complete spectra, including potential interferents (molecules with same molecular mass and similar electrical mobility).
The next relevant steps are the validation of the system in field tests.

Nuclear and Radiological (NR) detection

For the primary phase, NR detection relies on an already existing device, the RPM (Radiation Portal Monitor) and High Energy X-Ray.
For the secondary phase, the X-Ray image will be analysed for High Z objects or High density alarm, producing alarms inspected by the muon scanner, generating a 3d matrix of the sensed densities, which will be displayed later in the graphical tool for the users.

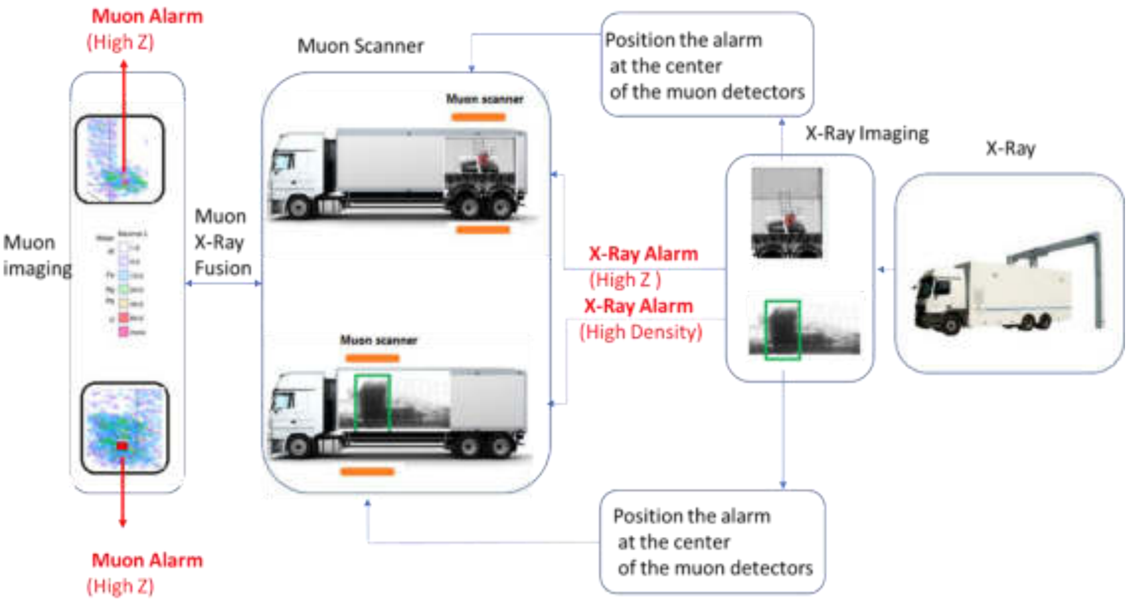


Figure 10. RN Detection using muon scanned. SOURCE COSMIC

The pilot of the muon scanner will be in Haifa seaport in 2021. The structure of the muon scanner pilot is shown in Figure 8. The scanner is based on two layers of muon detectors above the truck and two detectors layers below the truck.

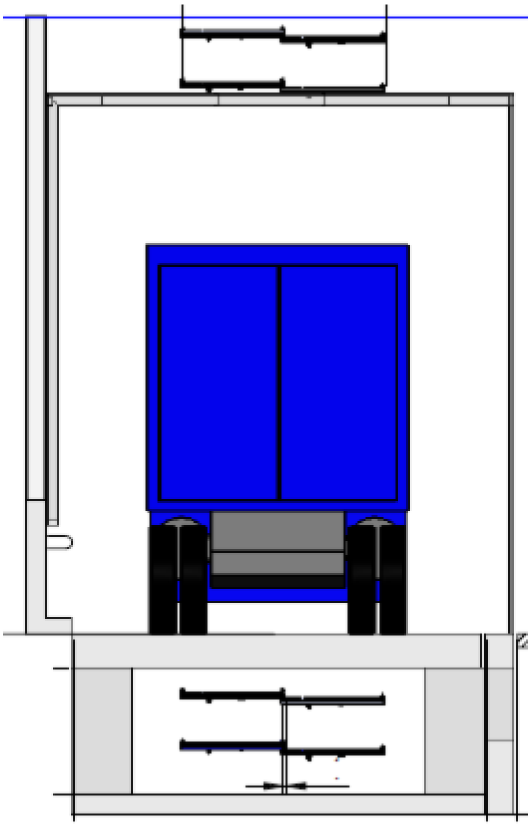


Figure 11. Pilot RN Detection using muon scanner. SOURCE COSMIC

Chemical and biological detection

DMS-MS: For primary phase a sensing unit based on GNPs chemoresistors sensor array is developed to provide initial alarm. The headspace taken from sample will be introduced to the array and data classification based on pattern recognition will allow alert on potential chemical\biological threat. For secondary same system will be used together with specific calibration curve that will be done to evaluate specific chemicals. Concept operation is illustrated in figure below.

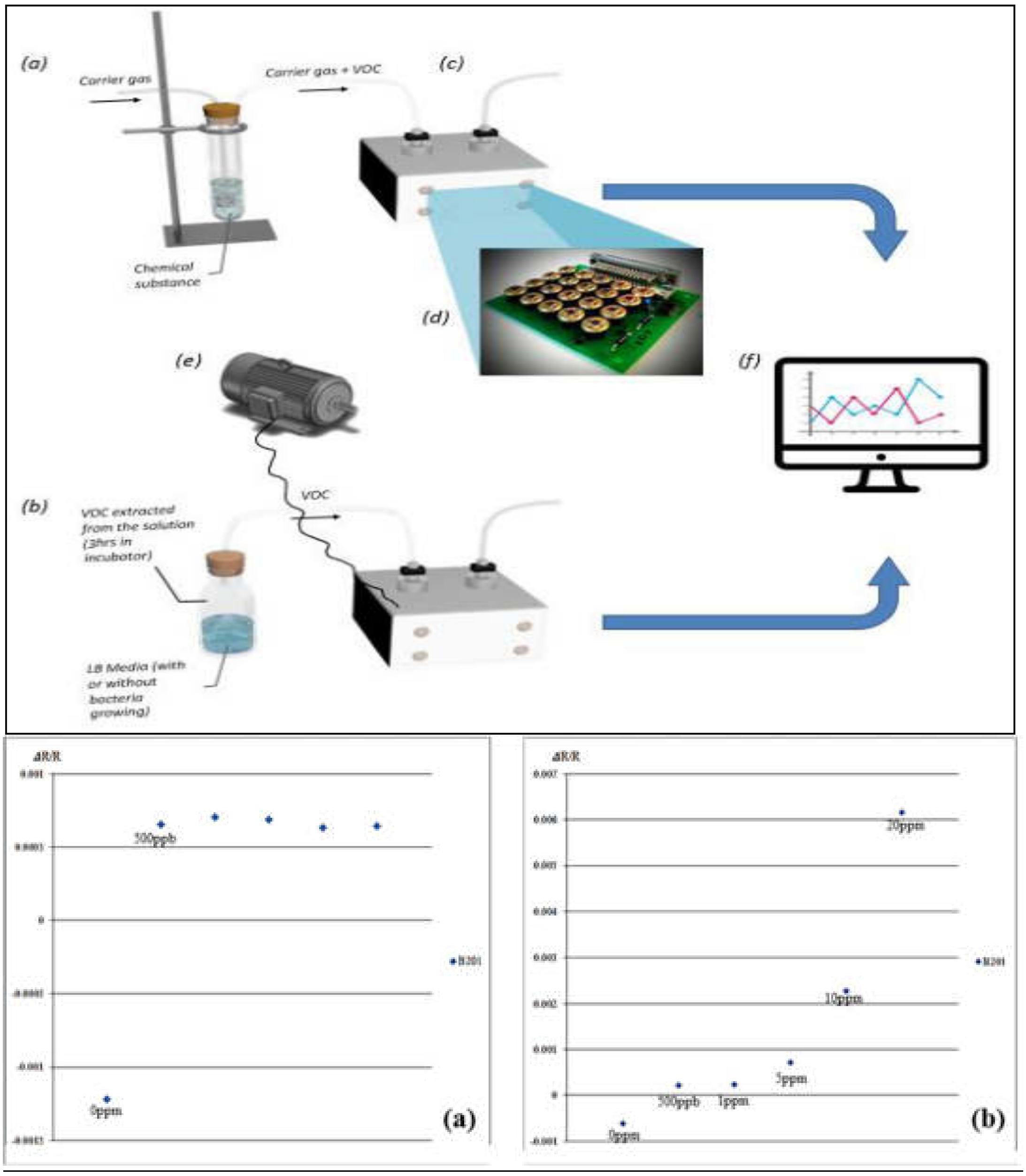


Figure 12. Nanose illustrative chemical and biological detection concept, (a)(b) selected sensor response in lab to Diethyl malonate, Soman simulant, Source COSMIC

On the other hand, the proposed DMA-MS instrument for explosive detection has been applied to the case of bacteria and chemical agents. The same vapour detection procedure as in the case of explosives has been applied, however the bacteria detection does not rely on the identification of an unique substance, but in the detection of a specific pattern of volatile compounds in very specific concentrations as it can be seen in the following figure where two types of bacteria have been unequivocally identified.

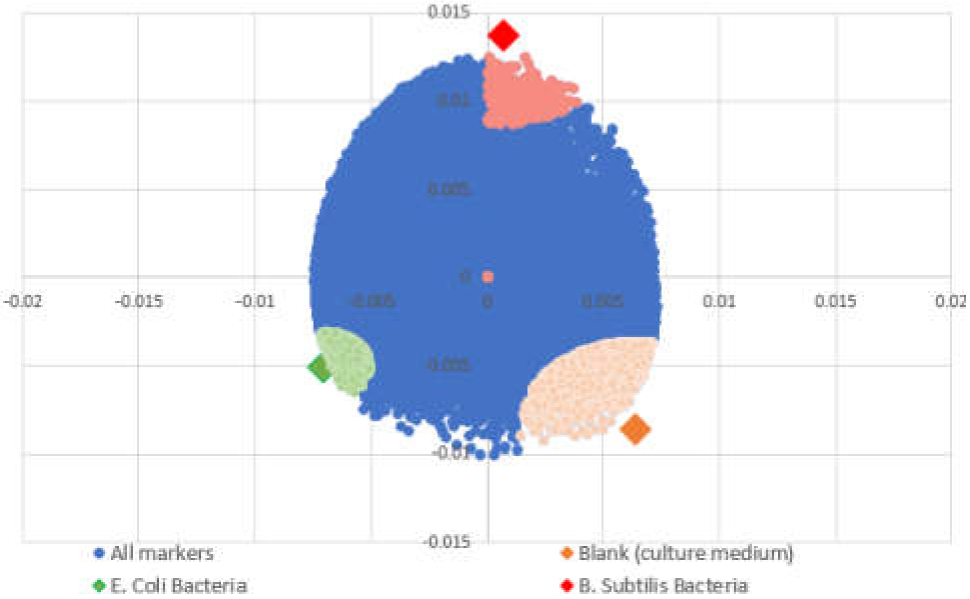


Figure 13. DMA-MS applied for bacteria detection: Source COSMIC

Improved DMA: COSMIC project, in collaboration with Yale University, has provided an improved DMA labelled provisionally as “PerezDMA”. The project has addressed some issues from previous versions and implemented solutions, improving the resolution of the instrument achieving a resolution of 4,37% (22,9) using the Israeli Acute Paralysis Virus (25 nm) as the following figure represents. This improved resolution compared to typical instrumentation (GEMMA) also allowed the study of different techniques of sample preparation. An iteration process of 3 steps of dialization provided the maximum reduction of background signal.

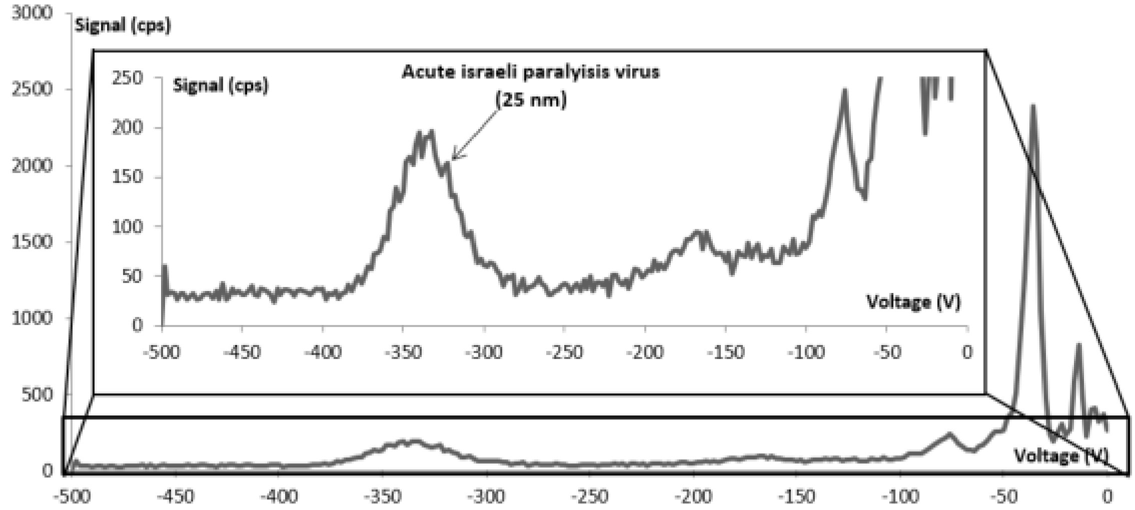


Figure 14. Detection of the Acute Israeli paralysis virus with the increased resolution and 3 step iteration of dialysis. SOURCE COSMIC

The consortium has developed a new version of the instrument with improved resolution (~50, which improves the ability of the instrument to discern a virus from another of similar size) and size range increased up to 400 nm. It is capable to analyse the SARS-CoV-2 (100nm), allowing to further improve the current sample preparation techniques due to its unparalleled resolution and also can act as a standalone detector capable of precisely discerning the presence of the virus particles.

PDA detection**:** BGU (Ben-Gurion University) focussed on the development of PDA configurations capable of detection of biological targets (bacteria) in varied settings, examination re. detection thresholds and required detection times. Optimization of sensing parameters and improving the integrated polymer/PDA platforms towards achieving higher performance led to construction of PDA prototypes.

By adding an amphiphilic dendrimer W3000 to TRCDA, we have a system in hand that is sensitive towards bacterial growth over time. We found that the optimal sensor for detecting the two bacterial strains studied was obtained by mixing 5:1 weight ratios of dendrimer and TRCDA. The solution was spin coated or drop casted onto a Perspex disc, dried and UV irradiated at 254 nm for 1 min to obtain the blue phase (polymerised DA), which has a shelf-life of at least 2 months, when placed in a well-plate with a lid. Bacteria at 2x dilution (OD 1 after overnight culture), when added to the system, can be detected after 2 h and 6 h for *E. coli* and *B. subtilis* respectively. The colour change from blue to red is visible and can be quantified with UV-Vis spectroscopy.

For the remainder of the project BGU will carry out analyses of sensor specifications in laboratory settings/ field trial simulations in the lab with different bacteria strains, creating a database comprising targets studied and concentration levels achieved.

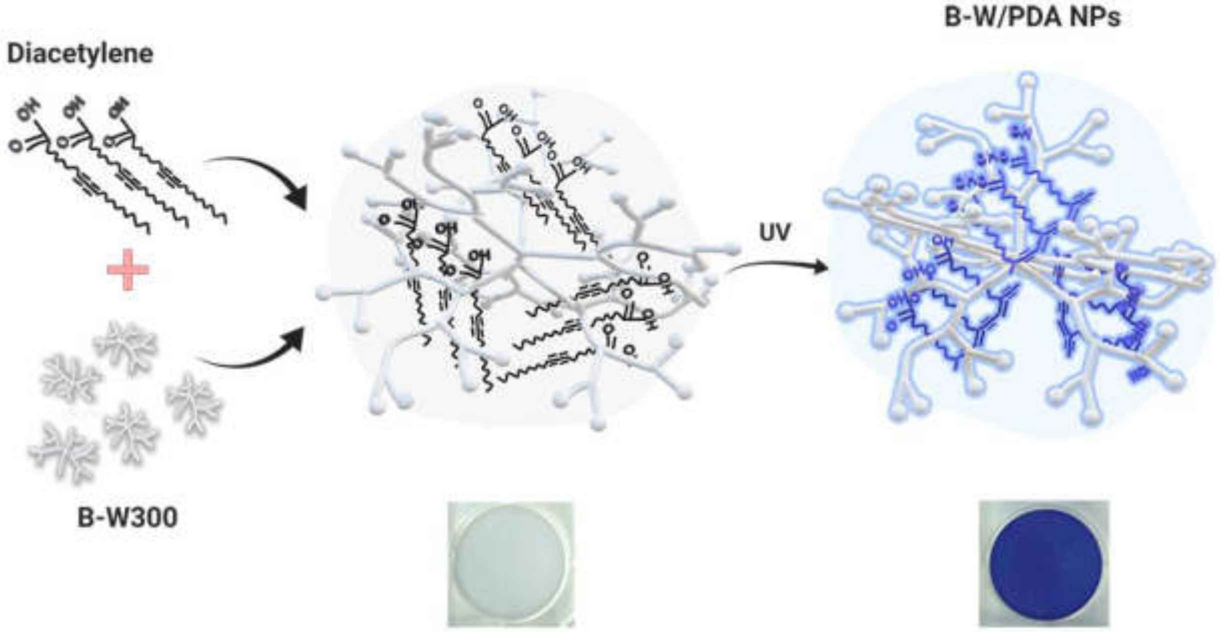


Figure 15. BGU PDA bacteria detection SOURCE COSMIC

2.5.3.2.2 Data fusion for combined sensor-profiling detection

Additionally to the physical sensors provided in the system, the project has developed the ability to provide logical sensors, which are software elements which combine the information of physical sensors, either with each other or with other sources of information, to produce a result that takes into account more information than the one used in a single sensor. More specifically, COSMIC is able to combine the data from the sensors with the information and the manifest and the experience of the system to refine the data from the physical sensors, resulting in refined detection.

For achieving this, COSMIC provides a neural network that combines the probability produced by each type of sensor with its nature and some specific fields of the manifest, resulting in a refined probability of detection.

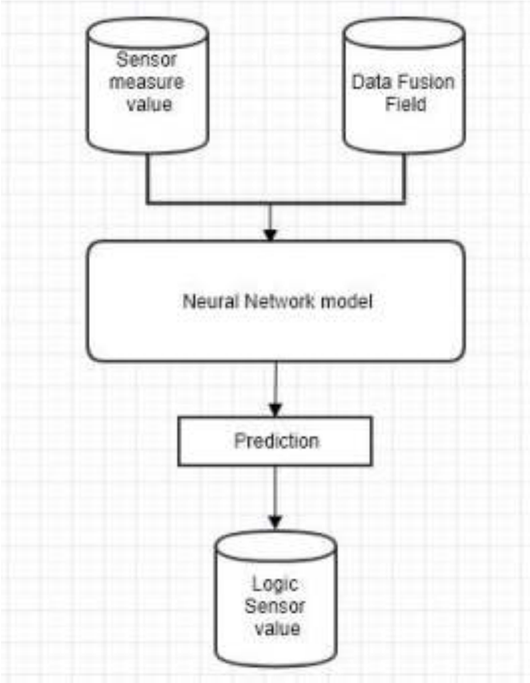


Figure 16. ATOS data fusion of sensor and manifest data SOURCE COSMIC

2.5.3.2.3 Graphical tool for the users

COSMIC provides a graphical tool that allows to easily perform the following operations:

- Access the summary of the manifest of each cargo for evaluating the risk of each container
- Graphically access the progress of each container in the system and the alarms produced in them including:
    - Current stage that the container is passing through
    - Icons that graphically depict the status for each kind of threat
    - Detail of all measurements taken for each container
- Manually input in the system the data for those sensors that due to their low-cost conception are not meant to send their data electronically to the system

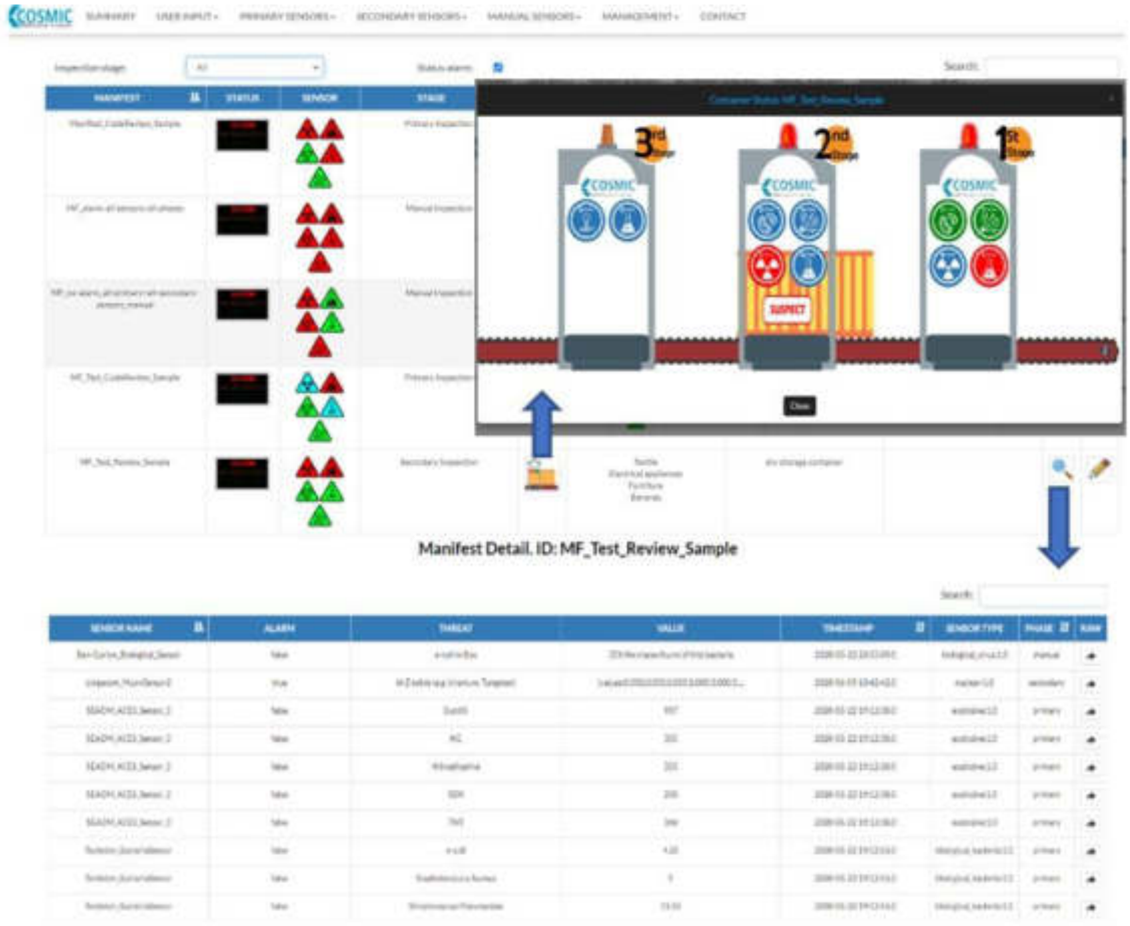


Figure 17. Screenshots of the COSMIC graphical tool (SOURCE COSMIC)

2.5.3.3 Benefits for the practitioners

Now practitioners can open those containers that trigger an alarm from the sensors jointly with their profile and devote their scarce resources to inspect only the most dangerous containers, resulting in an improvement in the smooth continuity of the release of containers from the customs. As suspect containers pass to different phases, letting the customs to continue the processing of the vast majority of containers, the new procedure should significantly contribute to avoid the congestion of the customs operation resulting from opening many suspicious containers.

2.5.3.4 Exploitation

Exploitation plans from the project and especially from the partners are constrained and for that reason cannot be published. However, some things can be revealed because they are public, such as:

- Industry partners have already contacted specific custom business lines to start marketing and promotion activities, resulting in contacts with several customs administrations in the European Union
- Active attendance to networking events, such as SRE or info-days to prospect potential stakeholders.
- Active collaboration with the ENCIRCLE project to gain visibility both among the research community and the potential customers.
- Inclusion in several solution databases related with CBRN detection in customs, including:
  - ENCIRCLE Catalogue of CBRNE solutions (http://encircle-cbrn.eu/catalogue/)
  - PEN-CP catalogue of customs solutions (https://www.pen-cp.net/)

If you would like to know more about the COSMIC project, please visit the project website at https://www.cosmic-cbrne.eu/.

2.5.4 EU-RADION

The EU-RADION project is a joint operation of 8 European institutions with varied fields of operation ranging from research facilities, through academic entities, to governmental bodies. The members of the consortium are focused on developing a novel system for CBRN threat detection and elimination that is set out to significantly improve the capabilities and safety of the first responders and emergency response teams.

The development process reaps the benefits of not only a wide range of experience and knowledge of the consortium members, but also from a close cooperation with potential end-users voicing their needs and suggestions during multiple workshops and consultation sessions throughout the duration of the project to ensure an impactful finished product with a real application.

The project is focused on designing and developing a fully operational system for detection and identification of RN materials with the added value of improved situational awareness and safety of the on-site personnel and dispatch teams. At the conceptual stage, the members of the project consortium have established the following High-Level Objectives to serve as a reference point for the work carried out under the project:

High-level objective 1 - To cover selected capability gaps of European first responders and CBRNe practitioners indicated in ENCIRCLE catalogue and IFAFRI study by development of relevant technologies,

High-level objective 2 - To enhance situational awareness of first responders/CBRNe practitioners during preparedness and response missions,

High-level objective 3 - To boost European CBRNe market innovativeness and support its competitiveness,

High-level objective 4 - To showcase the operational EU-RADION solution to first responders, CBRNe practitioners and European stakeholders in relevant conditions.
In order to achieve that, the EU-RADION consortium is focusing its efforts on providing both hardware and software solutions tailored to preparedness and response actions of practitioners in the RN domain.
The main components of the system in terms of hardware are as follows:

a) **Sensor Integration Unit** (SIU) – A modular device supporting wireless connection and comprising 3 sensors (Geiger counter, Cadmium Zinc Telluride (CZT) detector, gas sensor) allowing the SIU to identify the agent and the radiation dose rate. Each unit is adapted to both stationary and mobile (person-worn or mounted on unmanned ground vehicles called UGVs) operation, which allows to create a tight-knit network able to monitor any given area thoroughly and reliably. As a result of a consultation with the potential-end users, each unit will be powered by a non-proprietary, easily replaceable power source, which can be replaced with off-the-shelf batteries.

b) **UGV Swarm** – A novel solution in terms of situational awareness in a form of three unmanned ground vehicles of which 1 is controlled remotely by a qualified operator and 2 are moving autonomously in relation to the remotely controlled one and constantly adjusting their movement in order to scan a larger area in a much shorter time. Each UGV will be equipped with an SIU and a navigation unit with a positioning module, which would allow for unmanned probing of the environment, which is especially useful when there is a suspicion of high radiation dose rates in the area of interest (AOI)/ incident zone.

c) **Navigation Unit** – A tracking module that is based on both inertial and GNSS sensors developed to allow for determining precise location and navigation of the on-site personnel and EU-RADION assets. A tool that will significantly increase the real capabilities of dispatch teams and operators directly translating to improved efficiency and safety of the operation.

In terms of software, the main components are:

a) **Unified Data Model** – Developed on the solutions from the EU-SENSE project in order to provide interoperability and scalability of the network system. The proposed standard is based on XML files allowing for network configuration flexibility and is necessary for the initial setup of the entire network.

b) **Tactical Command Tool (TCT)** - The highest layer of the system serving as an intuitive user interface and integrating data from measurement and computational components. It will display a map display of the area of interest with georeferenced information of the system components, estimated hazard and source areas, offer means of commanding of the system elements along with a display of their technical status.

c) **Dispersion Modelling** – A novel technological solution able to handle complex geometry along with particle-inherent properties (density, spatial dimensions, static forces) in order to perform deposition simulations beyond standard modelling tools. It will allow for improved source estimation by application of adjoint dispersion models and the method of regularisation, with adaptation of parameter selection methods not yet used in these types of applications, e.g. Unbiased Predictive Risk Estimation, Generalised Cross-Validation and Discrepancy Principle.

The successful development of the abovementioned solutions will directly translate to a significant improvement in terms of not only effective and time-efficient operation of dispatch teams and emergency management bodies, but more importantly, it will result in providing much safer working conditions for the first responders and on-site personnel.
Implementation of the EU-RADION's results will allow for a more thorough monitoring of the area of interest. The process of detection and identification of dangerous CBRN materials will be performed with the use of the following sensors:

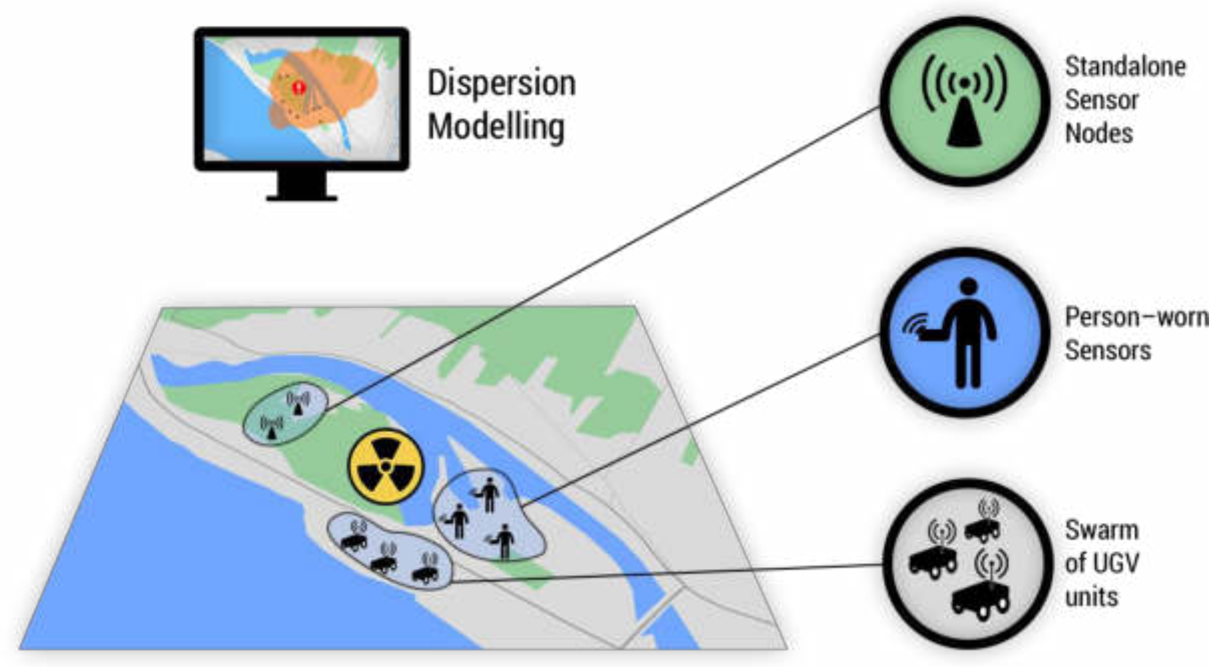


Figure 18. Detection and Identification - SOURCE EU-RADION

a) **Stationary**:
   - Cadmium Zinc Telluride and gas sensors supported by a Geiger counter
   - Implemented positioning module
   - Non-proprietary battery or AC power supply (depending on available infrastructure)
   - Wireless communication (processed data are displayed in the TCT)

b) **Person-worn**:
   - Cadmium Zinc Telluride and gas sensors supported by a Geiger counter
   - Implemented positioning module
   - Non-proprietary battery
   - Dedicated User Interface and display
   - Wireless communication (processed data are displayed in the TCT)
   - Generates alerts when close to detected hazards (based on threat map in TCT)

- Mobile collection of data

c) **UGV-mounted**:
   - Cadmium Zinc Telluride and gas sensors supported by a Geiger counter
   - Implemented positioning module
   - Non-proprietary battery
   - Wireless communication (processed data are displayed in the TCT)
   - Mobile collection of data

Using a combination of the abovementioned sensors will allow to paint a full picture of the area of interest and, with the use of the Dispersion Modelling software developed in the project, determine the exact area of the threat as well as its source and type. Moreover, this three-way approach provides more safety to the on-site personnel either by alarming them directly of the proximity of the threat (alerts on the person-worn sensors) or by keeping them away from the threat by sending the UGV swarm to monitor the area instead.

With a unique combination of multiple detection technologies, various sensor applications, and novel software, the EU-RADION system is bound to revolutionise the CBRN threat detection market and significantly improve the safety and efficiency of the emergency operators.

2.5.5 SERSING

Despite sustained efforts over the past decade or more, there has yet to be developed effective instrumentation for detecting and guiding responses to CBRN threats in public spaces. The SERSING (Exploiting Surface Enhanced Raman Spectroscopy (SERS) and Advanced Algorithms for Guiding Responses to Potential Chemical Threats) project entails the development of novel handheld or robot-mounted instrumentation for near-real-time or on-demand detection/identification of chemical threats coupled with advanced algorithms to aid responders and incident commanders in hazard assessment and decision-making. The SERSing concept is illustrated below. The handheld Raman spectrometer is equipped with surface enhanced Raman spectroscopy (SERS) add-ons that enable detection of chemical threats in gas and/or liquid phase. A more complex sample pre-treatment and identification of hazardous substances can also be performed on-site using e.g. disposable centrifugal microfluidic disc add-ons. The Raman-SERS devices can potentially be mounted on a robot for remote sampling and detection. The measurement results are then reported to an incident commander and displayed on a threat map.

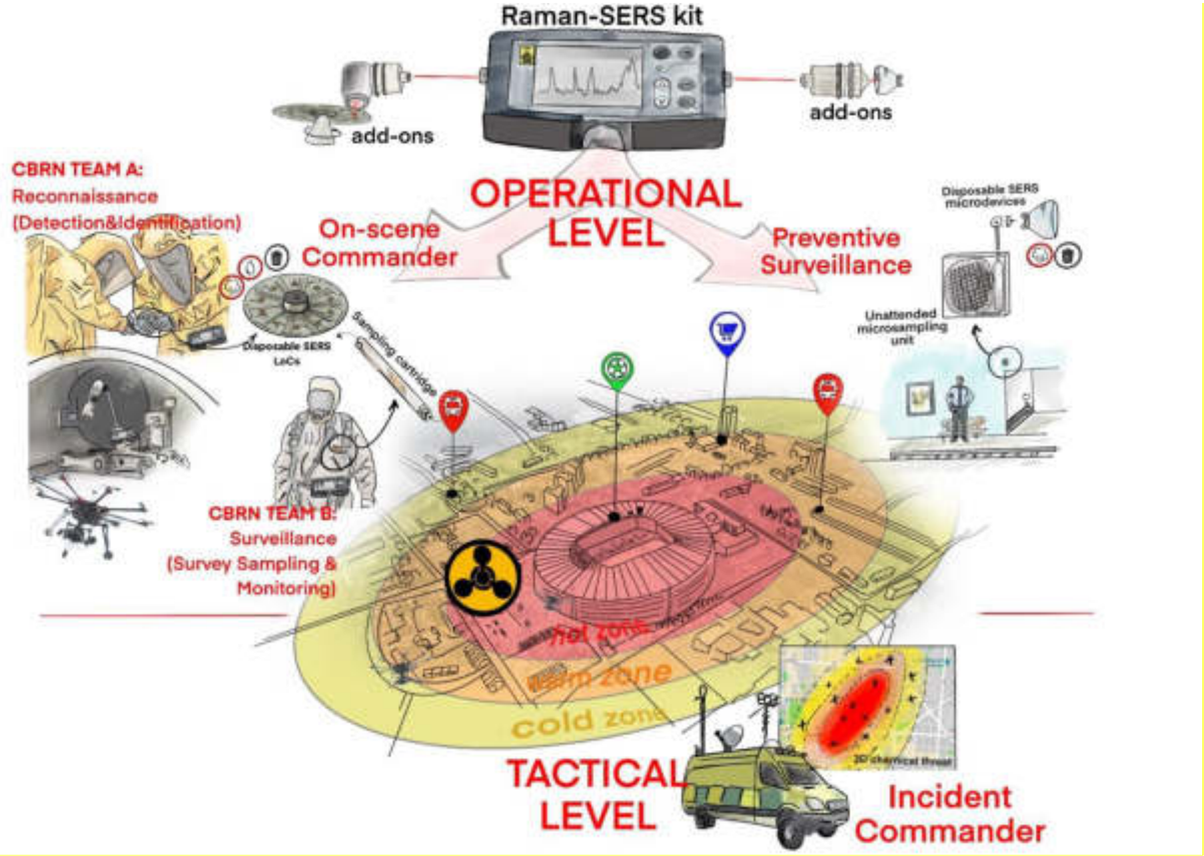


Figure 19. SERSING Concept: SOURCE SERSING

The SERSing project involves a team of four leading European academic groups, two high-tech companies (SME) with demonstrated expertise in advanced sensing and lab-on-chip (LoC) technologies, as well as two stakeholders (end users) responsible for CBRN and civil protection.

The vision and the overall goal of the project encompass a novel class of robust, lightweight, miniaturized, simple to use and cost-effective "plug and play" microfluidic surface enhanced Raman spectroscopy (SERS) platforms, which upon interrogation by an adapted handheld Raman spectrometer are able to provide a timely comprehensive picture of chemical hazards at the incident scene to improve real time situation awareness and decision-making (Figure 1). Gas and liquid samples are collected and delivered to the microfluidic platforms on demand or by a triggering signal; SERS analysis is performed and chemicals identified rapidly; and results are fed into a remote monitoring station equipped with fusion algorithms that provides options for response/action, if necessary. We have coined the term "SERSing" to represent this new SERS based approach (**S**ensing, **E**valuating, **R**esponding, **S**ecur**ing**).

The main objective of the SERSing project is to develop and validate "on field" for relevant chemical threats, i.e. chemical warfare agents (CWAs) and toxic industrial chemicals (TICs). The Raman-SERS Kit will be comprised of ultrasensitive SERS LoCs configured as ready to use "add-ons" for gas and liquid sampling and detection and a customized Raman instrument equipped with geo-location and communication technologies for the rapid screening of the incident scene. The Raman-SERs kit is conceived to overcome the common operational limitations of first responders, compatible with Personnel Protective Equipment PPE and respirators, easy to use and maintain with low cost of consumables. Thus, SERSing gives response to some of the existing capability gaps and specific needs already identified by ENCIRCLE[6] (European CBRN Innovation for the Market Cluster project, co-funded by the European Union's Horizon 2020 work program under grant agreement No. 740450, topic SEC-05-2016-CBRN cluster: Part a) and IFAFRI[7] (International Forum to Advance First Responder Innovation) in the domain of chemical threats.

The 2017 EU CBRN Action Plans to enhance preparedness against CBRN security risks (COM(2017) 610) and support the protection of public spaces (COM(2017) 612) emphasizes the need to strengthen Chemical Security with a focus on preparing for, and responding to chemical incidents and terrorism attacks. The tactical importance arises from shorter response times, shorter on-site assessment times, and faster recovery and restoration times. Research and innovation is essential to keeping up with evolving security needs.

According to the International Forum to Advance First Responder Innovation (IFAFRI), first responders need technologically advanced tools and equipment that are affordable and innovative to rapidly identify, detect and analyse threats and hazards. These solutions may also include subsequent software or devices enabled to display data and analysis on an intuitive user interface. In order to improve responder safety, efficiency and effectiveness, responders need the ability to i) rapidly identify hazardous agents and contaminants; ii) understand pertinent information regarding protective actions or treatments for these threats to improve response situational awareness at incident scenes and decision-making.

The commonly used cumbersome chemical detectors are mostly based on ion mobility/mass spectrometry techniques and their acquisition prices start from 30.000$ excluding data libraries. More specific detection based on immunoassay techniques does not cover the full spectra of evolving chemical threats. Miniaturized sensors are gaining of importance but efforts on multi-sensor integration and analyses are still required to provide with reliable measurements.

The successful project yields a rugged, easy-to-use, handheld Raman-SERS kit that can be operated by first responders wearing personal protective equipment, mounted on a robot/drone, or emplaced at a network of fixed locations. The instrument(s) can provide fast, trace-level detection and unequivocal identification of a wide range of chemical threats in air or liquid media encountered in real-world environments. The geo-located data are transmitted to a smart, on-line platform for rapid processing, and the information derived from the data is immediately accessible to authorized personnel for decision-making and response actions/alerts. The pre-operational validation of the prototypes by means on field exercises is also addressed to provide input for the iterative and continuous upgrading of the SERSing technologies. Commercialization is facilitated by involvement of SMEs and end-users throughout the development, implementation and outreach phases of the project.

[6] ENCIRCLE project (co-funded by the European Union's Horizon 2020 work program under grant agreement No. 740450, topic SEC-05-2016-CBRN cluster: Part a). Accessed on June´19: https://www.encircle.eu/

[7] The International Forum to Advance First Responder Innovation. Capability Gap 3 "Deep Dive" Analysis Synopsis. September 2017. Accessed on June´19: https://www.dhs.gov/publication/st-frg-international-forum-capability-gap-3-deep-dive-analysis-synopsis.

Project Update—March 2021 (Month 9)

The SERSing consortium met virtually on September 9th to officially kick-off the project. They focused initial efforts on finalizing important ethics documentation and establishing a thorough data management plan. A project website and social media accounts have been set up for external project communication to stakeholders and the public.

WP 1: Operational review in chemical threats DIM, SERS technology verification & proof of concept demonstrations (FOI)

FOI and SJUCHBO are working on detailing the overarching requirements of the device and creating scenario-driven reports to drive development. FOI has held in-person meetings with End User groups, as well as EU project RADION, to elicit feedback on the design and implementation of their end-product. They strongly emphasized that the final product must be very easy to use. At the scene of incident, the operators often wearing protection equipment, cloths and gloves, and they are (almost) always working under time pressure. It can be difficult to handle small objects and complicated instruments. To highlight this issue they suggested a “one button instrument” (that of course also is very robust and reliable). Though they understand it is very difficult to realize a one button instrument. However, it is important for the SERSing consortium to keep this in mind during the project in the strive to develop useful sensor devices aimed for the end users, i.e. it must be easy-to-use. Field tests are planned in CA/DoW for April-June 2023 and Sep-Dec 2023.

WP 2: Plasmonic substrates for SERS detection (UNIZAR)

The objective of WP2 is to develop outperforming SERS substrates for “on field” Raman detection of chemical warfare agents and toxic industrial compounds. Particular efforts are devoted to improve limit of detection, signal uniformity and response time when dealing with chemical threats in gas phase. A new PhD student (MSc. Kissia Batista) has joined the group on Feb´21 to work in this WP. Regular meetings between Unizar-UVigo, and Unizar-UTwente-SIL are being held.

Unizar is synthesizing and characterizing different plasmonic nanoparticles and their deposition onto solid supports. The strategy consists of the combination of adsorptive and molecular sieving properties of porous materials and plasmonic metals in a single nanoparticle. This will result in an increase of selectivity and sensitivity. The detection capabilities of the fabricated SERS substrates in our lab and by Silmeco and UTwente are been characterized using as probe molecule DMMP (dimethyl methylphosphonate) and CEES (2-chloroethyl sulphide), simulants of gas sarin and mustard, respectively.

On the other hand, numerical simulations based on the Finite-Difference Time-Domain (FDTD) method have been conducted of the SERS response of microsize pyramids fabricated by UTwente and optically characterized at INMA. We found that structures with around one micron size are better for SERS applications. First calculations to figure out the optimal configuration (pyramid size, pitch, metal thickness...) have been done, which show interesting benefits in the SERS enhancement process from both localized plasmonic resonances and surface plasmonic resonances.

During these months, UVigo has been working in the synthesis of plasmonic nanoparticles mainly Au, Ag or core-shell Au@Ag with tailored optical properties for the fabrication of high efficient sensing platforms. Thus, we have developed a novel green strategy to obtain Au nanostars (very efficient for SERS). Besides, employing a strategy reported previously by our group we have prepared core-shell Au@Ag nanorods coated within a ZIF-8 shell (sieving properties) to text their sensing capabilities. Experiments perform in liquid phase as well as in gas phase (performed by UNIZAR) have demonstrated their good performance for SERS detection of DMMP (dimethyl methylphosphonate) and CEES (2-chloroethyl sulphide), simulants of gas sarin and mustard, respectively.

Moreover, we have performed computational calculations (semiempirical and DFT) calculations to investigate different aspects of the DMMP diffusion and trapping inside the ZIF-8 cell as well as the type of interactions occurring between DMMP and metal surface. It will be crucial to understand the trapping effect of ZIF-8 as well as to analyse the SERS signals obtained.

SIL has been further developing surface-enhanced Raman scattering (SERS) substrate nanofabrication procedures. The focus is high-performance Au or Ag coated silicon (Si) nanopillar SERS substrates that could potentially be mass produced at low cost. The goal is to address common SERS substrate performance reproducibility issues and improve shelve life. The current strategy involves focusing on producing SERS substrates on 6” Si wafers, which would lower the substrate fabrication costs. The approach could be further extended to 8” Si wafers. At this point, the results show that 6” Si wafers yield a usable SERS-active area of approximately 75 cm^2. The next step is to reduce the SERS signal intensity variation across the wafer and reduce the background signal, which is important for reliable detection of target molecules at extremely low concentrations.

WP 3: Microfluidic SERS units for DIM of chemical threats in gas and liquids (DTU)

Based on the input from WP1, DTU is looking into different approaches when designing and fabricating microfluidic SERS modules. The End-user feedback collected by FOI outlines the need for ease of use, simplicity and automation. DTU currently is verifying the electrochemically assisted SERS-based detection of target molecules in liquids – a method that is simple, could be automated and miniaturized for integration with hand-held Raman spectrometers provided by Serstech AB. By applying a potential (approx. -0.4 – 0.4V) on gold or silver coated silicon nanopillar SERS substrates, target molecules can be attracted towards the metal film, and the SERS signal intensity significantly increases. Electrochemically assisted SERS detection is a viable pathway that we continue to explore.

WP 4: Artificial intelligence for DIM of chemical threats (DTU)

This WP involves close collaboration between DTU Compute and Serstech AB. Currently, the effort is focused on programming languages and types of communication. DTU Compute has assigned a PhD student (Bo Li) to work on the WP who is investigating data analysis options, theoretical considerations and requirements within the field. A plan for information sharing and training with the SERSTECH ´s Raman instrument has been created. Decisions in relation to hands-on training at SERSTECH is pending due to travel restrictions. Discussions and information sharing on algorithms has been initiated. Regular meetings are being held between SERSTECH and DTU.

WP 5: SERSing detection tools for first responders (SERSTECH)
A plan for assigning internal resources has been made.

WP 6: Project Management & Dissemination (SILMECO)
In addition to the project kick-off meeting, the SERSing consortium meets quarterly via teleconference to connect and discuss project progress.

Information about the SERSing project and updates can be found at sersing.eu. Follow us on twitter for the latest news: @SERSing_H2020

The project is coordinated by Dr. Tomas Rindzevicius of Silmeco ApS, in collaboration with 8 partners across Spain, The Netherlands, Denmark, Sweden, and the Czech Republic. Partners include: Technical University of Denmark, University of Zaragoza, University of Vigo, University of Twente, Serstech AB, Swedish Defence Research Agency (FOI), The National Institute for Nuclear, Chemical and Biological Protection (SÚJCHBO).

2.5.6 Other Projects and Initiatives

Physical collaborative efforts with other projects and initiatives has been disrupted over the last period due to the COVID crisis, but the following table highlights some of the virtual activities

Project	Progress
COU	Supported workshops and meetings for the development of the new COU including the COU in September 2020 and the DRS COU scoping meeting November 2020
eNOTICE	Market analysis questionnaires
FIRE-IN	Market analysis questionnaires and standards initiatives, and FIRE-IN virtual meeting June 2020

EXCERTER	Virtual meeting November 2020
NO-FEAR	Market analysis questionnaires and standards initiatives, collaboration with Stair4Security
EU- HYBNET	Project cooperation meeting May 2020
IFAFRI	Attendance of IFAFRI meeting June 2020
ILEA-NET	Innovation meetings November 2020
Network of practitioners	Market analysis questionnaires, virtual updates of ENCIRCLE and the Part B projects. ENCIRCLE webinar on the dynamic catalogue July 2020
STAIR4SECURITY	Virtual meetings on the Stair4security platform, and standards
STRATEGY	Strategy workshop Nov 2020

Figure 20. Collaborative projects list

2.5.7 List of ENCIRCLE Resources

Resources Include:

Public deliverables		
Resource	Description	Location
Part B 2019	Call Topics	ENCIRCLE Project CORDIS
D4.1	ENCIRCLE Cluster Discussions Y1	ENCIRCLE Project CORDIS
D4.2	ENCIRCLE Cluster Discussions Y1	ENCIRCLE Project CORDIS
D4.3	ENCIRCLE Cluster Discussions Y3	ENCIRCLE Project CORDIS
D4.4	ENCIRCLE Cluster Discussions Y4	ENCIRCLE Project CORDIS
D5.1	ENCIRCLE Cluster Impact Y1	ENCIRCLE Project CORDIS
D5.2	ENCIRCLE Cluster Impact Y2	ENCIRCLE Project CORDIS
D5.3	ENCIRCLE Cluster Impact Y3	ENCIRCLE Project CORDIS
	ENCIRCLE Cluster Catalogue 1	ENCIRCLE Project CORDIS
	ENCIRCLE Cluster Catalogue 2	ENCIRCLE Project CORDIS
	ENCIRCLE Cluster Catalogue 4	ENCIRCLE Project CORDIS
	ENCIRCLE Cluster Catalogue 6	ENCIRCLE Project CORDIS
	ENCIRCLE Cluster Catalogue 8	ENCIRCLE Project CORDIS
	Part B 2017 Call Topics	ENCIRCLE Project CORDIS
	Part B 2018 Call Topics	ENCIRCLE Project CORDIS

	Part B 2019 Call Topics	ENCIRCLE Project CORDIS
Newsletters and Magazines		
Resource	Description	Location
Magazines	ENCIRCLE Issue 1, 2, 3, 4	ENCIRCLE Website
Newsletter	ENCIRCLE Newsletter 1,2,3	ENCIRCLE Website
Information available in the ENCIRCLE Catalogue – Networks and Groups Forum		
Resource	Description	Location
Business Maturity Model Template	Template for business modelling	ENCIRCLE Resources Folder
Market Analysis	Market analysis reports and surveys	ENCIRCLE Resources Folder
ENCIRCLE Discussion	ENCIRCLE Discussions reports	ENCIRCLE Resources Folder
Toolkit	Draft toolkit to support SME led projects	ENCIRCLE Resources Folder
2020 Needs and Gaps List	Consolidated Unclassified CBRN Needs and Gaps - draft	ENCIRCLE Resources Folder
Human Factors Analysis and Reports	Summary of the Human Factors questionnaire Analysis and individual reports, including COVID	ENCIRCLE Resources Folder
Integration	Integration guidelines report	ENCIRCLE Resources Folder
Standards	CBRN consolidated standards worksheet	ENCIRCLE Resources Folder

Figure 21. Encircle resources

2.6 PLANNED ACTIVITIES IN 2021

Planned activities in 2021 include

Event	**Activity Type**	**When/Where**
DRS COU on CBRN	Virtual Meeting or workshop	May 19th 2021
iProcureNet workshop	Virtual	March 9th 2021

Stair4Security workshop	Virtual	May 2021
Project Completes		September 2021
New Cluster		September 2021

2.7 ENCIRCLE SUSTAINABILITY

The following text summarises the latest discussions and thoughts in the area which are still under development and reflects feedback received to date:

2.7.1 ENCIRCLE Website

The ENCIRCLE website, which also provides link to ENCIRCLE Dynamic Catalogue, will be maintained in its current form by WAT for a period of at least two years after the project completes at the end of August 2021. Before the end of the ENCIRCLE project website will be updated with the information regarding ENCIRCLE results and achievements and other information including updates on new projects and other R&D activities in CBRNe field.

2.7.2 ENCIRCLE Catalogue

The ENCIRCLE catalogue will be maintained in its current form by UNS for a period of two years after the project completes at the end of August 2021. Before the end of the ENCIRCLE project the intention is to get in place a new neutral management board in place by August 2021.
The Networks and Forum facility in ENCIRCLE will be closed at the end of the ENCIRCLE project, and the ENCIRCLE resources will be published and available on CORDIS by project end.

2.7.3 Innovation Watch

The Innovation Watch will be maintained in its current form by EU-VRI and will be supported until March 31, 2023.

2.7.4 DRS04 Part B Project Support

As part of the support of the DRS04 projects, for when the ENCIRCLE project finishes, a toolkit is being prepared of the ENCIRCLE resources to support these projects. This toolkit will be available in the Network and forum resources folder whilst the project is active, and move to CORDIS when the project completes.

2.7.5 ENCIRCLE Cluster

A number of options are being explored concerning the sustainability of the cluster. These include the potential progression of ENCIRCLE into a new CBRNe thematic working group as part of the future Community of European Research and Innovation for Security (CERIS).

As part of this activity the following process is inspired by discussions with DG HOME on how a practical implementation of a Capability Based Approach in the field of security and in support to security research planning could look like. The recently published EU action plan on synergies between civil, defence and space industries[8] also specifies a capability driven approach for security "ACTION 1: Before the end of 2021, the Commission will present a proposal to strengthen the forward-looking and early identification of needs and solutions in the field of internal security and law enforcement by fostering capability-driven approaches across security sectors, building on best practices from the defence and space sectors"

It should be noted that the following approach does not reflect any actual or planned implementation, but is just a conceptual model that could serve as a reference for a potential future workflow that could be supported by CERIS. The following diagram from DG HOME illustrates a high level capability based research cycle process and the subsequent sections described how the ENCIRCLE Cluster could evolve to provide continuation of the existing capabilities. This will be further refined during the period to August 2021 including consideration of how pop up threats/fast track innovations should be included.

[8] https://ec.europa.eu/info/sites/info/files/action_plan_on_synergies_design_v9_en.pdf

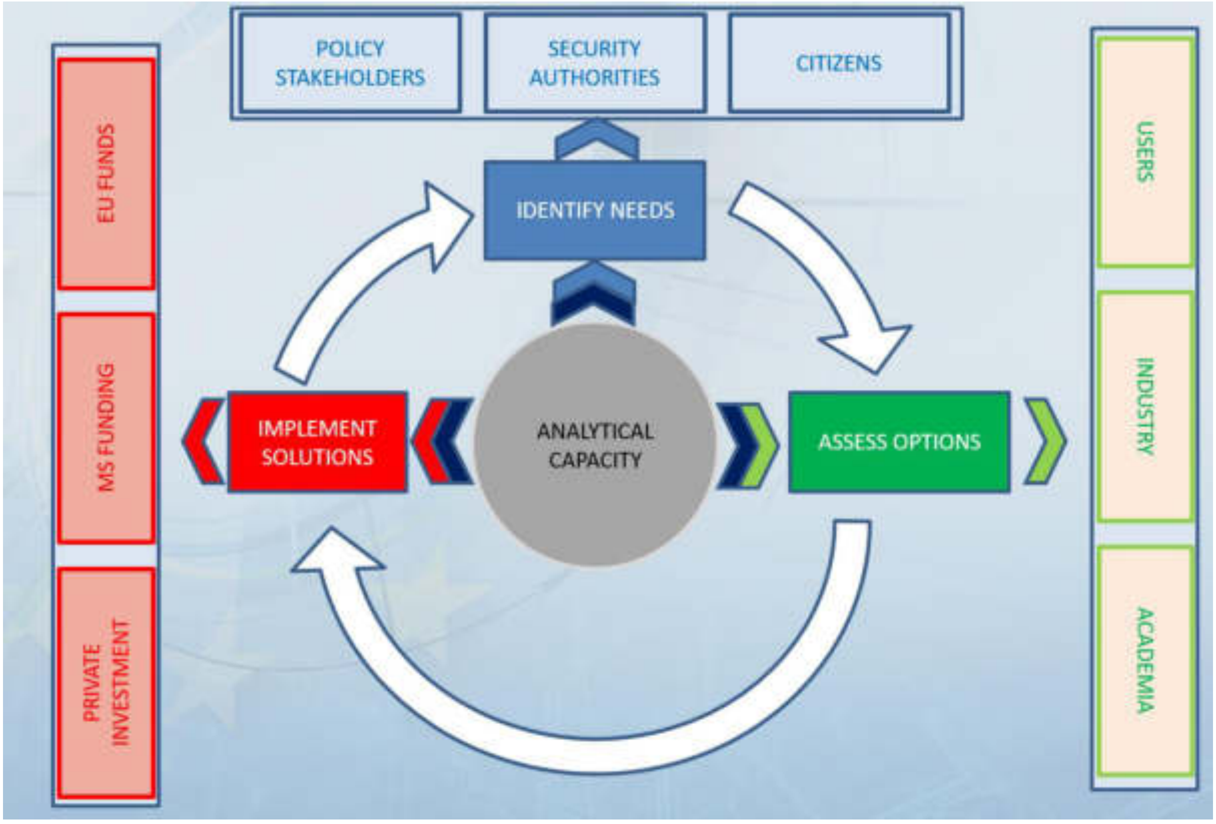


Figure 22. Capability Planning Model (SOURCE DG HOME)

The three individual process steps (Identify Needs, Assess Options, Implement Solutions) are illustrated further with a high-level description of the activity and the process steps

2.7.5.1 Identify Needs

- This process step takes into account policy priorities, and the future threat landscape and conducts a capability assessment to define capability gaps and a capability development plan.
- As part of the capability assessment there are a number of constraints that are taken into account. These include whether the solution assessed in the Assess Options stage has resulted in a solution that is not value for money, and the results of the operational reviews of deployed capability.
- As part of the capability plan development as well as the capability gaps to be closed, and additional input concerns whether there are any European sovereign capability needs and constraints for the development of such capability.

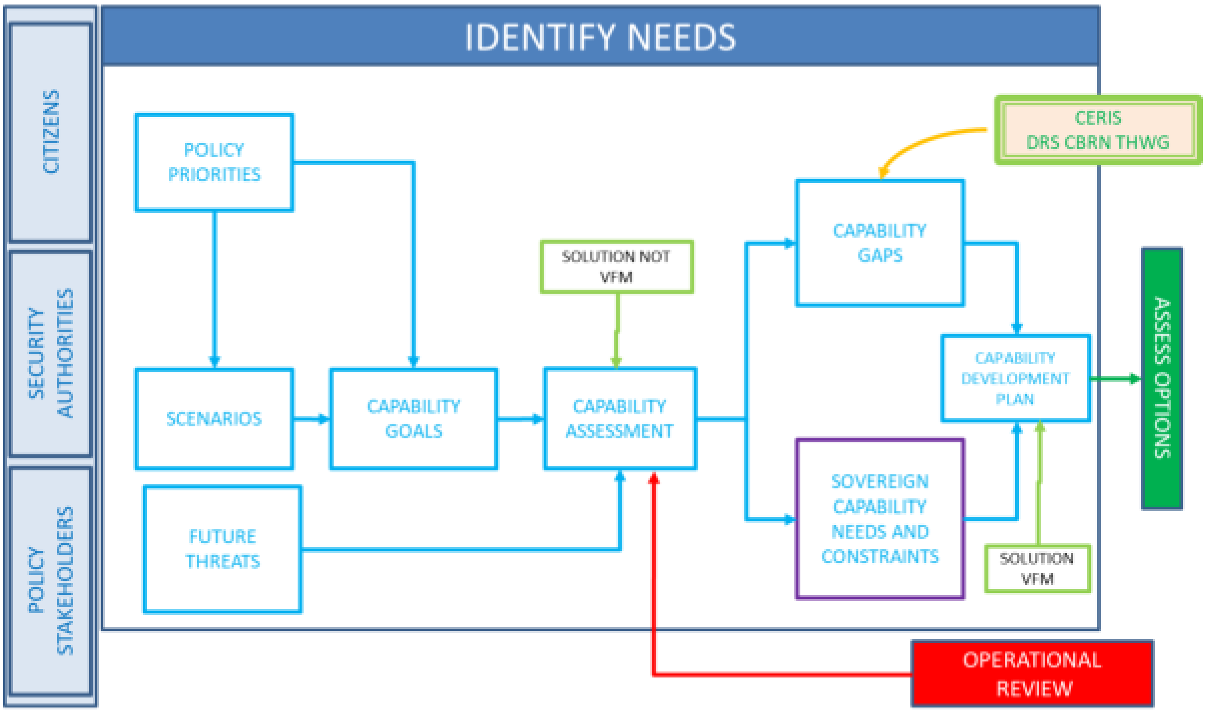


Figure 23. Identification of Needs

Process	Description	Input/Output
Policy Priorities	Policy priorities for CBRN such as the CBRN Action plan	Input: Policy requirements Output: Any policy priorities against time
Scenarios	Scenarios of the types of tasks expected to be undertaken	Input: Real time/generic scenarios, policy priorities Output: Prioritised scenarios
Future Threats	An up to date assessment of the future threat landscape	Input: Threat Intelligence Output: Rated Threats against time
Capability Goals	What are the capability goals to meet the policy priorities and scenarios	Input: Scenarios, Policy priorities Output: Prioritised capability goals
Capability Assessment	An assessment of the capability goals to be addressed against the future threat landscape and current operational capabilities that have been deployed	Inputs, Capability goals, Future threats, whether solutions are value for money and the results of the operational view of deployed solutions. Output: Capability Assessment
Capability Gaps	Identification of capability gaps that need to be addressed	Inputs: Results of capability assessment Outputs: Gaps that need to be met over time
Sovereign capability needs and constraints	A consideration on whether there needs to be any EU Sovereign capability	Input: Capability Assessment Output: EU sovereign capability constraints

	constraints for development or acquisition	
Capability Development Plan	The generation of a capability development plan against time	Input: Capability gaps and sovereign capability constraints Output: Capability Development Plan

2.7.5.2 Assess Options

The assess options process stage includes a state-of-the-art assessment and prioritisation process and then an assessment on whether the solution is affordable.

- The State of the Art assessment takes as its inputs:
  - The capability plan from the Assess Needs process
  - The outputs of the innovation watch activity
  - The outputs of other mission areas or domains which may have sovereignty constraints on technology deployment, operation and maintenance
- The output of the process step is
  - A prioritised list of potential solutions and requirements in terms of
  - Criticality
  - Urgency
  - Maturity
  - Resources
  - And Sovereign constraints
  - A value for money assessment is then conducted which if successful will then enter the implementation stage

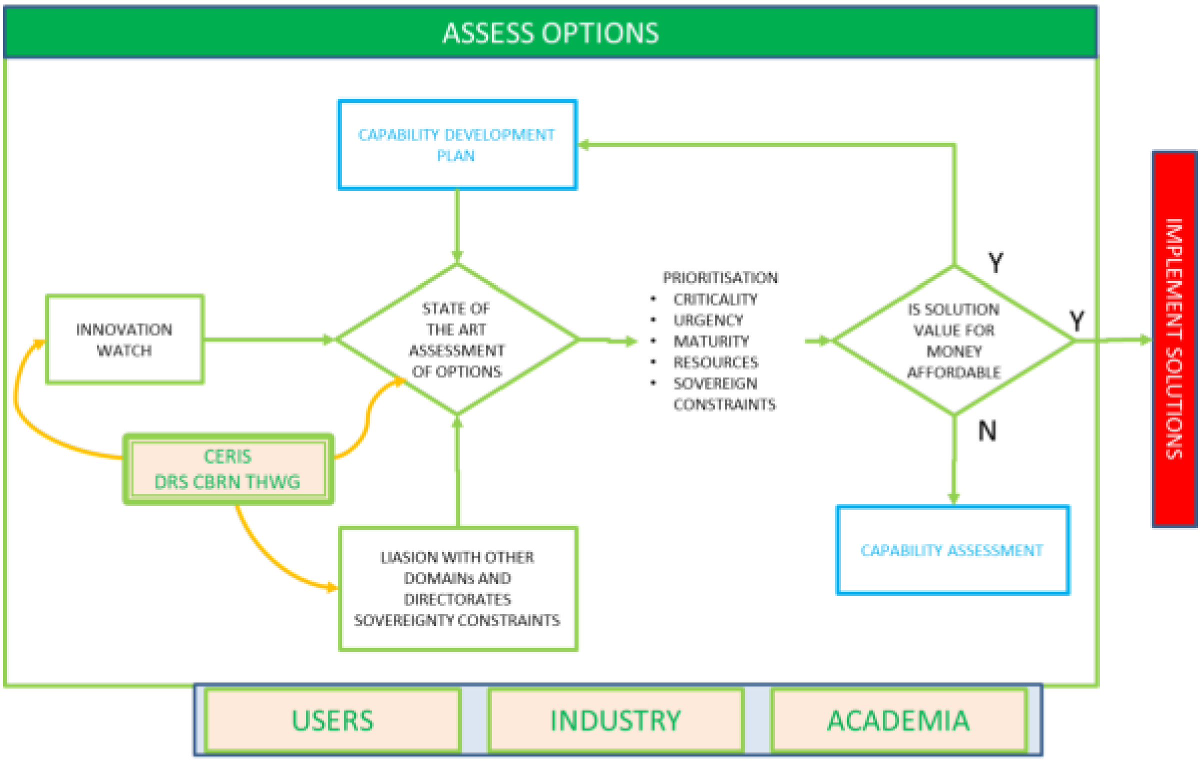


Figure 24. Assess Options

Process	Description	Input/Output
Innovation Watch	An innovation watch on new technology and process developments	Input: Output: Up to date catalogue of potential solutions (Technological and Non-technological)
Liaison with other domains and directorates sovereign constraints	Checking with other domains and directorates on whether they have any EU sovereignty constraints for cross-cutting technology and process developments that need to be considered by this domain	Input: Constraints from other domains and directorates Output: Relevant constraints on cross-cutting technologies and process solutions,
State of the art assessment of options	An assessment of the outputs of the capability plan against potential solutions (technology/process) to meet the plan and any constraints	Input: Capability plan, constrains from other directorates and domains and potential solutions Output: A prioritised list of potential solutions in terms of: Criticality, Urgency, Maturity, Resources and Sovereign constraints
Prioritisation		Output: The priority list

Is Solution value for money	Conducting a value for money assessment, if successful then solution can enter the implementation stage and capability plan is updated, if not back to the capability assessment	Input: Prioritised list Output: Yes or no decision to implement the solution with a number of options and constraints, or go back to the capability assessment

2.7.5.3 Implement Solutions

This process step takes the outputs from the Assess Options stage and assesses whether.

- the identified solutions are in the market.
- could be developed from state-of-the-art innovations.
- or whether a new research and innovation project is required.

Depending on the answers to these questions the development and integration process is initiated, and then acquisition and deployment.
As a final step an operational review is conducted on the deployed solution which provides feedback back into the Needs process.

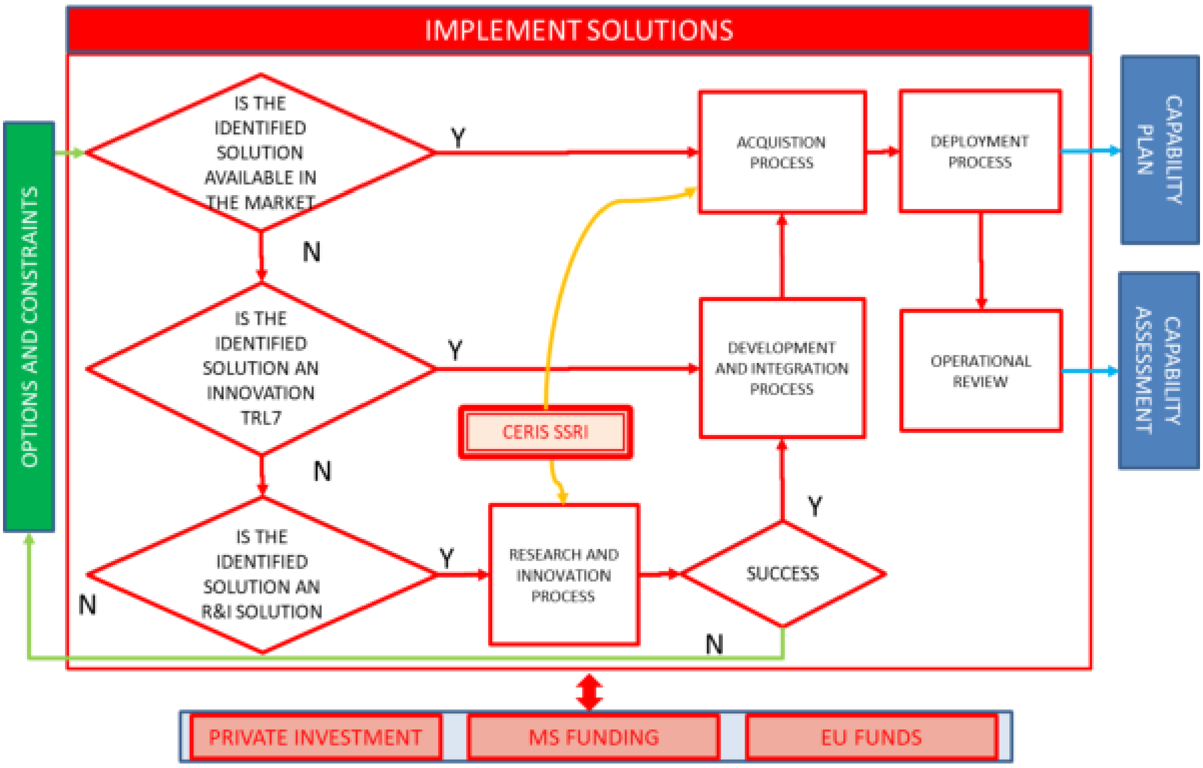

IMPLEMENT SOLUTIONS
OPTIONS AND CONSTRAINTS
IS THE IDENTIFIED SOLUTION AVAILABLE IN THE MARKET
Y
N
IS THE IDENTIFIED SOLUTION AN INNOVATION TRL7
Y
N
IS THE IDENTIFIED SOLUTION AN R&I SOLUTION
Y
N
ACQUISTION PROCESS
DEPLOYMENT PROCESS
DEVELOPMENT AND INTEGRATION PROCESS
OPERATIONAL REVIEW
CERIS SSRI
RESEARCH AND INNOVATION PROCESS
SUCCESS
Y
N
CAPABILITY PLAN
CAPABILITY ASSESSMENT
PRIVATE INVESTMENT
MS FUNDING
EU FUNDS

Figure 25. Implement solutions.

Process	Description	Input/Output
Is the identified solution available in the market	A check to see if the solution is available in the market	Input: Options and constraints Output: Yes acquire, No check whether solution can be developed with SOA technology
Is the identified solution an innovation >TRL6	A check to see if a solution has a maturity greater than TRL6	Input: No solution available in the market Output: If Y go forward with development and integration, if No solution required R&I
Is the identified solution an R&I solution	A check to see if Research and Innovation is required	Input: a No from no solution in market or innovation available Output: Y – enter research and innovation process,
Research and Innovation Process	The research and innovation process to mature the solution or a maturity level of TRL7. This should undergo stage gate reviews to ensure the development is viable	Input: Capability needs and requirements including policy, standards and integration and interoperability requirements and constraints. Output: Results of R&I project at TRL 7
Success	A checks to see if the project has met the needs	Input: Output of Research and Innovation process Output: Yes proceed to develop, No – Assess options
Development and integration process	Maturation to TRL 9	Input: TRL6 solution Output: TRL 9 solution
Acquisition process	Acquire the solution	Input:TRL9 solution, Output, Solution acquired
Deployment process	The solution is fully deployed, including support and training	Input: acquired Solution, Output, capability deployed
Operational Review	Assessment on whether the deployed solution met the need	Input: Operational feedback, Output: Assessment on whether the deployed solution met the need

2.7.5.4 ENCIRCLE Cluster evolution

The final diagram summarises how the ENCIRCLE Cluster could evolve to support a capability planning process and support a new version of the Community of Users by evolving the capabilities into two working groups.

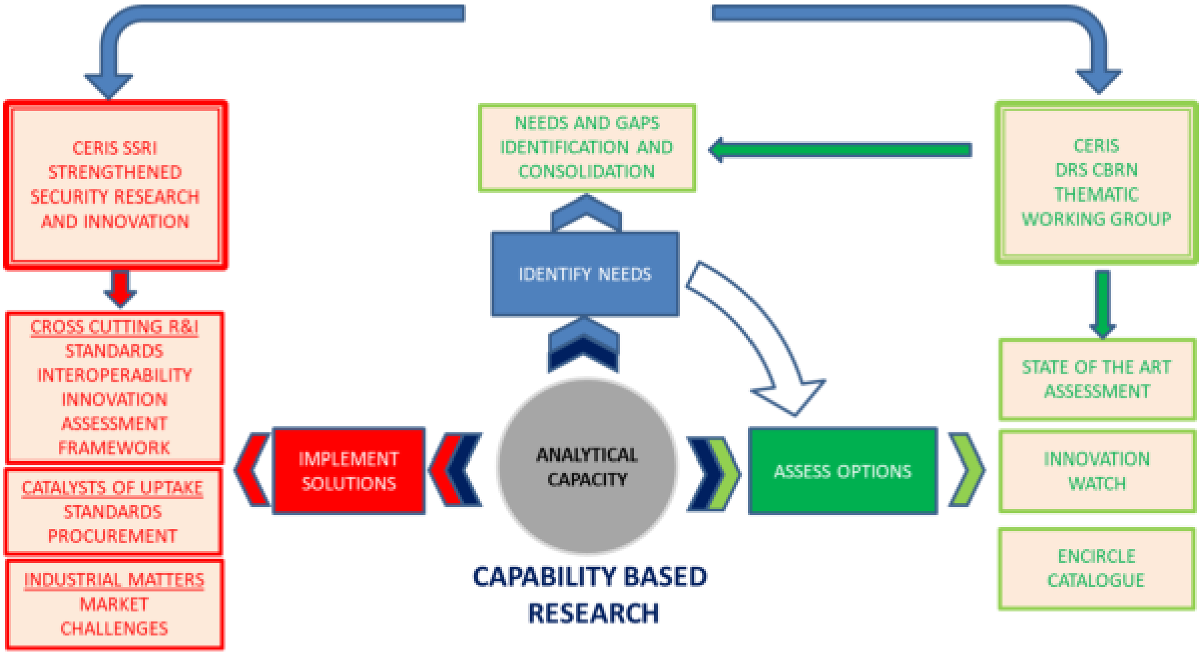


Figure 26. CBRN Thematic working Group

3 ENCIRCLE IMPACT

The following table summarises the impact of the ENCIRCLE project to date to shorten the time to market for novel CBRN technologies and innovations against the project objectives.

Impact		Status
a	Provide an early identification of needs and markets for new innovations	The needs and gaps from the EDEN project have been updated and relationships are in place with the practitioner networks. These needs and gaps have been prioritised for the DRS calls in collaboration with the practitioner and technological communities and DG HOME. The ENCIRCLE market surveys have provide an early indication in the change of needs such as the increased emphasis on the biological threat and the improvements required for information management and DIM
b	Provide early identification of new products and innovations	The ENCIRCLE Dynamic Catalogue contains nearly 250 registered organisations and nearly 300 tools. The innovation watch resource is operational and includes an "innovation watch" widget which presents potential interesting novel innovations and a "radar" widget that provides a pre-analysis on on-going developments in the field of CBRN. Recommendations for future portals are contained in the Impact Y4 Annex 2 - Results of the ENCIRCLE's developments impact analysis.
c	Support better exploitation of previous and current innovation projects, including orphan results, through identification and facilitation of the most appropriate financial instruments,	Links to financial instruments to support innovations are available on the ENCIRCLE project site. ENCIRCLE has been working with TERRIFFIC, COSMIC and EU-SENSE in supporting their innovations and tool kits are being put in place to support the 2019 and 2020 projects when the ENCIRCLE project finishes. As part of the project support IPR assessments and business maturity assessments have been made to start to support their needs A number of discussions have also been conducted with ENCIRCLE partners and two SME Part B for potential future cooperation
d	Provide recommendations to fill/meet important gaps through the Part b calls,	The recommendations for the topics to be included in the 2017, 2019 and 2020 DRS Call were successfully completed. This included a lessons

		learnt exercise after the 2017 call for the 2019 and 2020 calls.
e	Provide improved and easier integration and interfaces between research results and products and existing practitioner and user systems, by sharing commercial efforts and access to market between SME and large industries cooperating in the cluster	An integration report has been produced and an interface and standards collection and assessment exercise has been conducted. Within the ENCIRCLE Resources on the network and forum Resource site the latest integration report and standards database can be found. A Market analysis was conducted and is also posted in the ENCIRCLE Dynamic Catalogue Network and groups forum in the resources folder. In 2020 an updated market analysis has been conducted which considers Needs and gaps, standards, procurement, policy and the market and this will be available October 2020 in the same repository.
f	Speed up the European CBRN innovation capacity by its open, standardised interfaces and its portal facilities (catalogue, community network, market place)	Interfaces to allow better integration of CBRN solutions were collected and workshops conducted in 2019. Recommendations have been made for more standardised communication protocols and for Civil Protection symbology to aid integration and interoperability. The ENCIRCLE Dynamic catalogue includes functions for the catalogue, community and market place.
g	propose innovation topics that will meet the significant market current and forthcoming needs for the Part b call	The 2017, 2019 and 2020 calls have all been successfully completed
h	speed up the European innovation capacity in CBRN through the use of standardised interfaces. The integration of new knowledge will be included in the Portal (catalogue, expert network and market)	Interface and standard information have been collected, policy, procurement and market analysis surveys have all been conducted and analyses and the results presented at the COU's and documented in the ENCIRCLE Market Analysis reports. Deliverable (ENCIRCLE Cluster Impact Y4 Annex 1 – provides the results of the analysis of the legal documents concerning security and defence procurement and provides recommendations.

Figure 27. ENCIRCLE -Impact Summary

4 ANNEX 1 SECURITY AND DEFENCE PROCUREMENT ANALYSIS

ENCIRCLE

EuropeaN Cbrn Innovation for the maRket CLustEr

D5.4 ENCIRCLE Cluster Impact Y4 Annex 1 - Results of the analysis of the legal documents concerning security and defence procurement

This publication only reflects the view of the ENCIRCLE Consortium or selected participants thereof. Whilst the ENCIRCLE Consortium has taken steps to ensure that this information is accurate, it may be out of date or incomplete, therefore, neither the ENCIRCLE Consortium participants nor the European Community are liable for any use that may be made of the information contained herein.
This document is published in the interest of the exchange of information and it may be copied in whole or in part providing that this disclaimer is included in every reproduction or part thereof as some of the technologies and concepts predicted in this document may be subject to protection by patent, design right or other application for protection, and all the rights of the owners are reserved.
The information contained in this document may not be modified or used for any commercial purpose without prior written permission of the owners and any request for such additional permissions should be addressed to the ENCIRCLE coordinator.

Dissemination level

PU	Unrestricted PUBLIC Access – EU project	**X**
PP	Project Private, restricted to other programme participants (including the Commission Services) – EU project	
RE	RESTRICTED, Restricted to a group specified by the consortium (including the	

	Commission Services) – EU project	
CO	Confidential, only for members of the consortium (including the Commission Services) – EU project	

Document Information

Grant Agreement n°	**740450**	
Project Title	EuropeaN Cbrn Innovation for the maRket CLustEr	
Project Acronym	ENCIRCLE	
Project Coordinator	Université catholique de Louvain (UCL)	
Document Responsible Partner	Grzegorz Kowalski (PIAP)	grzegorz.kowalski@piap.lukasiewicz.gov.pl
Document Number	D5.4	
Document Title	ENCIRCLE Cluster Impact Y4 Annex 1 - Results of the analysis of the legal documents concerning security and defence procurement	
Dissemination Level	Public	
Contractual Date of Delivery	Month 48 (09 March 2021)	

Partners involved in the Document

N°	Participant organisation name (short name)	Check if involved
1	**Université Catholique de Louvain (UCL)**	
2	BAe SYSTEMS (BAES)	
3	Ouvry SAS (OUVRY)	
4	Sieć Badawcza Łukasiewicz - Przemysłowy Instytut Automatyki i Pomiarów PIAP (PIAP)	**X**
5	Tecnoalimenti (TCA)	
6	Wojskowa Akademia Techniczna (WAT)	
7	European Virtual Institute for Integrated Risk Management (EU-VRi)	
8	Istituto Affari Internazionali (IAI)	
9	Université de Nice-Sophia Antipolis (UNS)	
10	Universita Cattolica del Sacro Cuore (UCSC)	
11	FALCON COMMUNICATIONS LIMITED (FALCON)	
12	Smiths Detection Watford Limited (SMITHS)	
13	MIKKELIN KEHITYSYHTIO MIKSEI OY (MIKSEI)	
14	ENVIRONICS OY (EOY)	
15	ADS GROUP LIMITED LBG (ADS)	

Circulation list

- European Commission
- ENCIRCLE Consortium

EXECUTIVE SUMMARY

This document presents the results of the analysis of the legal documents concerning security and defence procurement at European and Member State level. The main goal of this analysis was to indicate the amount of obligations, that have to be fulfilled by the technical supplier of governmental agencies, who provides technology, products and services for police and military purposes to governmental agencies responsible for public and national security – fire service, police, border guards, armed forces. This report presents the most important and difficult obligations, that have to be fulfilled.

The supplier, who wants to be part of security and defence procurements, depending on the nature of the product/service, has to be acknowledged not only with general rules on conducting business activities with local or foreign clients, but also with the rules on internal control system, export control system or protection of classified information and has to apply for a special permission to even offer “special equipment” when being only a broker. These many rules are separated onto number of legal documents. Twenty five documents from European and national (Poland) level have been identified and analysed. Part of them are the Directive and Regulations issued by the European Union’s bodies. They present the rules and obligations for the authorities or agencies carrying out purchasers for end-user supervised by Ministry of Internal Affairs or Ministry of Defence. Some of these rules are huge burden for the supplier, as he has to create or adjust its business to meet several requirements from fields like internal control system, classified information or export control. Some of them are quite easy to fulfil, but some requires making investments or apply for documents with a long period of waiting for granting. All these rules have to be fulfilled as the State can apply a penalty over not correctly carried out processes.

A1 Introduction

Technologies for the security and defence areas are special-purpose products, used by agencies and forces supervised by EU Member States' Ministries of Defence and Ministries of Internal Affairs – fire service, police, border guards and armed forces. Due to the fact, that these agencies and forces serve the public and country safety, their equipment should be characterized mainly by reliability and durability. This is the reason of putting such a focus on securing appropriate quality and safety of the production. Inevitable risk related with such equipment is its possible usage by unauthorized personnel or criminals and terrorists. For that reason, the special equipment is a subject to tight control, usually during its whole lifecycle.

Production, trade, storage and transport of special-purpose products and technologies have been controlled by governmental bodies supported by legal regulations defining general principles of these processes. General rules are provided by European level documents, usually in form of Directives. According to rules from the Directives they should have been be implemented in Member States' law. Some Member States have also introduced additional rules to tighten the control over the most specialized technologies that could be used as weapons against the society or the environment. Due to the fact that payments for such technologies are usually conducted by governmental agencies/bodies paying in public money, they fall under the rules of public procurement law or – in some cases of the procurement for armed forces – under special procedures concerning essential interest of the safety of the country.

This analysis provides the basic list of the European documents concerning production, storage, transport and procurement of technologies for security and defence. It also discusses some particular rules, that are very important or could be not obvious for the company new in such area. Having mentioned that there is also law on national level, this analysis lists the document from selected Member State – Poland – and, similarly to European documents, points out the most important and intricate rules. This analysis discusses documents concerning security and defence procurement but only mentions some of the general documents, that shall be known for every enterprise conducting economic activity. The recipients of security and defence technology are usually state units, representing formations like police, fire service, border guard, but also armed forces. The contractor – technology provider – can be either private business or companies owned by governmental bodies. Analysed documents present rights and obligations for both sides of the contract, to be fair for the contractor and to assure fulfilling of technical, safety and confidential requirements of the recipient. As this document's main goal is to help technology providers to introduce their products to the market, the analysis discusses only their obligations and rights.
All analysed documents have been accessed in various parts of 2018, 2019 and 2020, so the analysis is valid for the moment of acquisition of the documents. Some of analysed documents can be outdated – in these cases it is mentioned in the description. When using this analysis for business purposes one should confront its timeliness with the currently applicable law.

A2 The analysis of the legal documents

A2.1 General documents concerning procurement

Rules on commercial activities, that concern procurement, are presented in documents at both European and national levels. These documents describe conducting business in civil area with governmental agencies, so every company has to know their content in order to be compliant with the existing law.

European level main documents are:

- Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts[9],
- Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC[10],
- Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC[11].

Some documents at national level in Poland are:

- "Announcement of the Marshal of the Sejm of the Republic of Poland of October 3, 2018 on the publication of the consolidated text of the Act - Public Procurement Law"[12] (new version of this document will be available in 2021),
- "Announcement of the Marshal of the Sejm of the Republic of Poland of September 16, 2020 on the publication of the uniform text of the Act - Civil Code"[13],
- "The Act of May 28, 2020 Amending the Public Finance Act"[14],
- "Announcement of the Marshal of the Sejm of the Republic of Poland of October 8, 2020 on the publication of the uniform text of the Act on combating unfair competition"[15],
- *"Regulation of the Minister of Development of 26 July 2016 on the types of documents that the contracting authority may request from a contractor in a contract award procedure"*[16]*,*

[9] Available at https://eur-lex.europa.eu/eli/dir/2014/23/oj, multiple languages, access: 11th Dec 2020

[10] Available at https://eur-lex.europa.eu/eli/dir/2014/24/oj, multiple languages, access: 11th Dec 2020

[11] Available at http://data.europa.eu/eli/dir/2014/25/oj, multiple languages, access: 11th Dec 2020

[12] Available at https://www.uzp.gov.pl/__data/assets/pdf_file/0019/40177/Public_Procurement_Law_2018_consolidated.pdf, ENG, access: 15th Jan 2019

[13] Available at https://dziennikustaw.gov.pl/DU/rok/2020/pozycja/1740, PL, access: 11th Dec 2020

[14] Available at https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200001175, PL, access: 11th Dec 2020

[15] Available at https://dziennikustaw.gov.pl/DU/2020/1913, PL, access: 14th Dec 2020

[16] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160001126, PL, access: 14th Dec 2020

- *"Announcement of the Marshal of the Sejm of the Republic of Poland of 11 June 2019 on the publication of the consolidated text of the Act - Entrepreneurs' Law"*[17]*,*
- *"The Act of 6 March 2018 - Regulations introducing the Act - Entrepreneurs' Law and other acts related to business activity"*[18]*.*

Similar acts can be found in other Member States' laws. As mentioned in the introduction, this list is not full and some of the documents could have been updated since the creation of this analysis.

A2.2 Documents concerning conducting business activities in the field of production and trade of products for security and defence

In Poland, there are some documents at national level, that present rules on conducting business activities, that cover production, storage and trading of special products. The most important is "Act of 13 June 2019 on conducting business activities in the field of production and trade of explosives, weapons, ammunition as well as products and technology for military or police purposes"[19].

According to this document, it is necessary to apply for the concession for the production and trade of explosives, weapons, ammunition and other technologies for military of police purposes (art. 7.1). Granting a concession is paid by the supplier (art. 20). The list of these products and technologies is announced by the Council of Ministers in a regulation (art. 7.3). The newest version of this list has been published in "Regulation of the Council of Ministers of 17 September 2019 on classification of types of explosives, weapons, ammunition and products and technologies for military or police purposes, the production or trade of which requires a concession"[20]. It contains names or general descriptions of:

- explosives,
- weapons,
- ammunition,
- chemical and biological warfare,
- fire control equipment with its accessories,
- special ground vehicles,
- warships and their parts,
- manned and unmanned air vehicles with their accessories,

[17] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001292, PL, access: 14th Dec 2020
[18] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000650, PL, access: 14th Dec 2020
[19] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001214, PL, access: 14th Dec 2020
[20] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001888, PL, access: 14th Dec 2020

- other special purpose electronic devices not mentioned in previous parts of the documents,
- training equipment for military or police use,
- recording devices and detectors,
- direct energy weapon systems and their accessories,
- equipment using cryogenic or superconductivity phenomenon,
- products related to security of classified information,
- armoured equipment and constructions and their components,
- equipment and technologies for manufacturing of special products,
- other products for military and police use, not covered by previous part of the document.

The list shall be analysed as a whole, because particular device can be mentioned indirectly. For example, chemical detectors are mentioned directly, but the last part of the document mentions devices for detection and identification of chemical warfare agents. This list contains products, that are present in “Common Military List of The European Union” [21], but is less detailed. One can expect that the national list will be updated when the new European list is published.

The Act presents some rules on granting the concession. For example, the concession can be granted to a supplier, who is able to fulfil technical and organisational requirements to run weapons registration system (art. 10.2).

There are also some personnel-related rules. For example, employees involved in production or trading explosives and other technologies and products for police and military use have to have necessary medical and psychological examinations (art. 12, art. 28 and art. 29). First examinations are paid by the employee, another ones – by the employer (art. 32). If the supplier is a natural person, he should have Polish or Swiss citizenship or of foreign country from EU or EFTA or other country, when permanent residency or long-term EU residency has been granted (art. 10.1.1.a). Art. 11 states, that such supplier has to pass the training, mentioned in art. 10.1.1.d. Details of such training are presented in “Regulation of the Minister of Economy of 25 September 2002 on training confirming professional preparation to perform or manage a business in the field of manufacturing and trading in explosives, weapons, ammunition and products for military or police purposes, and trading in technology for this purpose”[22]. § 8 of this Regulation informs that the training is paid.

The Act puts some commitments for the supplier. For example, there is an obligation to implement a system for evaluation of production quality (art. 41.1). This system shall be later evaluated by designated institutions (art. 41.3), but such evaluation is paid (art. 41.5). Another obligation is described in art. 63, which states that the information about trading of some products shall be sent to appropriate authorities. The storage of the special products can be carried out in designated facilities in appropriate conditions (art. 33.1), described in art 33.2.

[21] Newest version available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2019_095_R_0001, multiple languages, access: 13th Jan 2021

[22] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20021731415, PL, access: 14th Dec 2020

Detailed requirements for the facilities are described in the particular regulation (art. 33.4). Applicable regulation is called "Regulation of the Minister of Economy of 27 October 2010 on storage rooms and facilities for the storage of explosives, weapons, ammunition and products for military or police purposes"[23]. According to art. 47 and art. 59 the supplier is obliged to keep records of produced special products and carried out trades. Details of this processes are described in "Regulation of the Minister of the Interior and Administration of October 30, 2019 on the recording of explosives, weapons, ammunition, products and technologies for military or police purposes as well as trade and brokerage transactions intended for trading and accepted for storage or in commissioning"[24].

The Act also regulates transfers of special products - they can be sold only to: contractors having suitable concession, national authorities from the field of security and defence and other contractors with suitable permissions (art. 61.8 and art. 61.10). It is not allowed to lend explosives, weapons or products and technology for military or police purposes (art. 68.1), except for test purposes, exhibitions and as a temporal replacement for particular entities (art. 68.2-3).

A2.3 Documents concerning security and defence procurement

Depending on the receiver, the deliveries of products for security area (usually agencies under ministry of internal affairs: police, fire service, border guard) and defence area (under ministry of defence) can be described in different documents. There are some general documents concerning trading of special products, but when the procurement is carried out by army, additional documents, issued by ministry of defence apply. Such situation has been noticed in few Member States' laws.

The most important document at European level is the "Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC"[25]. The rules from this Directive have been implemented into national Public Procurement Law. The Directive received several changes of financial

[23] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20102221451, PL, access: 14th Dec 2020
[24] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190002235, PL, access: 14th Dec 2020
[25] Available at https://eur-lex.europa.eu/eli/dir/2009/81/oj, multiple languages, access: 22nd Dec 2020, new version available at https://eur-lex.europa.eu/eli/dir/2009/81/2020-01-01, multiple languages, access: 22nd Dec 2020

thresholds, above which the Directive is applied (Commission Delegated Regulations: 1177/2009[26], 1251/2011[27], 1336/2013[28], 2015/2340[29], 2017/2367[30], 2019/1830[31]).

The rules of the Directive mainly apply to deliveries of military products, sensitive equipment, works, supplies and services connected with the mentioned products, works and services for special military purposes or sensitive works and services (art. 2), when procurement's value is equal of higher than EUR 420.000 net for supplies and services and EUR 5.548.000 net for construction works (according to art. 8 updated by Regulation 2019/1830). Although art. 11 says that it is prohibited to use treaties, procedures, programmes, etc. to omit the rules of the Directive, articles 12 and 13 present some rules when the Directive does not apply. Worth mentioning is art. 13.a, which says that the Directive does not apply when procurements following the rules could disclosure information about essential security of the Member State[32]. This exemption is a repetition from the art. 346 of the "Treaty on the Functioning of the European Union"[33]. Some other important and interesting rules of the Directive can be divided into following categories:

- classified information, internal control system[34]:
    - during gathering offers or granting the contract, purchaser may require solution aimed at protection of classified information when necessary, both from the contractor and its subcontractors (art. 7),
    - necessity of assurance of the protection of classified information if the contacts involves it (art. 22),
    - for the security of the supply, the contracting entity may require certain documents, like certificates or other documents, supporting e.g. fulfilment of the requirements of internal control system (art. 23),
- subcontracting:
    - contracting entity may require information about the potential subcontractors from the tenderer (art. 21.2),
    - proposition of subcontracting can be rejected by contracting entity with an explanation (art. 21.5),
- publication of offers:
    - the order cannot be partitioned to avoid applying of the Directive (art. 9.3),
    - purchase may not be announced when products are bought on particularly advantageous terms, e.g. from the company in closing period (art. 23.3.c),

[26] Available at https://eur-lex.europa.eu/eli/reg/2009/1177/oj, multiple languages, access: 22nd Dec 2020
[27] Available at https://eur-lex.europa.eu/eli/reg/2011/1251/oj, multiple languages, access: 22nd Dec 2020
[28] Available at https://eur-lex.europa.eu/eli/reg/2013/1336/oj, multiple languages, access: 22nd Dec 2020
[29] Available at https://eur-lex.europa.eu/eli/reg/2015/2340/oj, multiple languages, access: 22nd Dec 2020
[30] Available at https://eur-lex.europa.eu/eli/reg/2017/2367/oj, multiple languages, access: 22nd Dec 2020
[31] Available at https://eur-lex.europa.eu/eli/reg_del/2019/1830/oj, multiple languages, access: 22nd Dec 2020
[32] This case will be explained in the further part of this analysis
[33] Available at https://eur-lex.europa.eu/eli/treaty/tfeu_2016/art_346/oj, multiple languages, access: 22nd Dec 2020
[34] Internal control system is described in further part of this document

    - whole purchase notice is published in one language selected by the contracting entity. A summary of the most important elements of each notice shall be published in the other official languages (art. 32.4),
    - contacting entity may limit the number of participants in some procedures to minimum 3 (art. 38.3), but establishing the final number of participants is based on undefined subjective opinion of contracting entity,
- submission of offers:
    - offers shall be prepared in particular language (or languages) (art. 34.5.b-c),
    - submission deadline for offers can be shortened when certain conditions are fulfilled (art. 33.3-33.5, 33.7),
    - submission deadline for offers can be extended when the offers are based on a visit or on-site document inspection performed by the supplier (art. 33.6),
    - as a proof of technical capabilities, a list of supplies, construction works or services performed in the arbitrarily defined period of the last 5 years may be required (art. 42.1.a),
    - contractor can apply for including the company in the official lists of approved economic operators, which relieves the obligation to present certain documents when submitting offers (art. 46),
- selecting the offer:
    - offers that do not comply with the technical specifications cannot be rejected if the supplier will prove that the solution meets the requirements defined by the technical specifications in the equivalent way (art. 18.4),
    - there is no defined deadline for publishing of the results of the tender by the contracting agency (art. 35.1),
    - when the offer is abnormally low, the contracting entity may request the explanation of the details of the offer (art. 49.1),
- granting contracts:
    - during granting contracts the contracting entities follow national regulations compliant with this Directive (art. 25),
    - for technical reasons or reasons connected with the protection of exclusive rights, the contract may be awarded only to one particular contractor (art. 28.1.e),
    - granting a contract can be made only after rejected candidates have been noticed of rejection of their offer (art. 57.2),
    - in case of notification of the rejection of the offer using electronic means, notification deadline is minimum 10 calendar days (15 for other means) (art. 59).

In Poland, description of the security and defence procurement is included in “Act of 29 January 2004 – Public Procurement Law”[35], which presents rules for application of this Act to operations, that are excluded from public procurement when protection of essential

[35] Available at https://www.uzp.gov.pl/en, ENG, access: 5th Jan 2021; new consolidated version in Polish will be available in 2021

security interest of the State is required (art. 4.5.b, art. 4c and art. 5g). Procurements carried out by the Ministry of Defence under art. 346 of TFEU are described in the documents provided by the Minister of Defence and will be presented in the further part of this analysis. "Public Procurement Law" presents procedures, that have to be followed, among others, by the public agencies or other institutions while buying goods/services with public funds. Details are presented in art. 3. Art. 4 contains the list of exclusions of application of this Act. As the Act is mostly on general rules of public procurements, only the part applicable to security and defence area has been analysed.

In general, tenders are available for suppliers from EU Member States, European Economic Area (EEA) or countries with which Poland or EU has procurement agreements. Suppliers from other countries can be allowed when tender states so (art. 131d). For the security of the supply, the contracting authority may determine some commitments for the supplier (art. 131g.2), for example: delivery of documents confirming fulfilling requirements concerning exportation, transfer or transit of goods for security and defence procurement (art. 131g.2.1) or/and definition of restrictions concerning transfer or usage of the products and services (and their results) being the subject of exportation or security control (art 131g.2.2).
The Act presents some facilitations (for the supplier or procedure itself), for example:

- if it won't affect competitiveness, it is allowed to provide (if requested) documents of fulfilling the tender requirements on the products, from certification entities, accredited otherwise than stated in art 30b.2 (art. 131g.6),
- some types of procurement allow the purchaser to carry out procurement is phases, during which the best offers will be selected for the following phase (art. 131h.4).

There are also some limitations, for example:

- when less than three offers have been submitted to the bid purchaser can suspend or cancel the bid (art. 131j),
- the maximum amount of subcontracting is 30% of the offer (art. 131m.3).

There are also some rules on tenders involving classified information. Supplier must provide warranty on safety of classified information, when its transfer is necessary for carrying out the procurement process (art. 131f). The same applies to the subcontractors (art. 131g.2). If the supplier doesn't have the special office for processing classified information, the classified information can be shared in the reading room of confidential office of purchaser on condition that the supplier's representatives possess a security clearance according to provisions on protection of classified information (art. 131v.3).

Another important document at European level is the "Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community"[36]. This Directive presents rules

[36] Available at http://data.europa.eu/eli/dir/2009/43/oj, multiple languages, access: 14th Dec 2020, new version available at http://data.europa.eu/eli/dir/2009/43/2019-07-26, multiple languages, access: 14th Dec 2020

on intra-EU transfer of defence related products, which are listed in Directive's annex, which contains:

- weapons, their accessories and parts,
- ammunition and its components,
- bombs, missiles, explosives and related equipment,
- weapon control systems and their accessories,
- land vehicles and their components,
- chemical or biological toxic agents (e.g. warfare agents), radioactive materials, related equipment (e.g. personal protective equipment or detectors) and materials,
- high-energy materials,
- warships, special maritime equipment and other special maritime military equipment,
- manned and unmanned air vehicles, their equipment and components, related airborne equipment,
- special electronic equipment,
- kinetic weapon systems, related equipment and components,
- armoured and defence equipment, constructions and their components,
- special training and simulation equipment,
- military-grade electromagnetic detection devices,
- semi-finished products for the equipment mentioned in this list,
- other special equipment and materials (e.g. protection equipment, robots),
- devices for manufacturing of the products mentioned in this list,
- direct energy weapons, their accessories and related equipment,
- cryogenic and superconductive equipment and its components,
- specialized software (e.g. for simulation of weapons),
- specialized technology (e.g. for production of weapons).

This list corresponds with the "Common Military List of the European Union", which future updates will update the list in the Directive – according to art. 13.1.

The Directive presents rules mainly on granting licences for transfer of defence-related products, but also some obligations for the suppliers and authorities. All transfer of defence-related products, mentioned in the annex, have to be authorized by a Member State representatives. If there is no conflict with the rules of public safety, no other licences are necessary (art. 4.1). Authorisation of transfers is carried out using licences, that can be granted to suppliers (art. 4.4). There are three types of licences:

- general licence – for transfer of products, specified in the licence, to a category or categories of recipients located in other Member State (art. 5.1). It can be granted in the following cases (art. 5.2-3):
    - the recipient is armed forces or has got a certificate mentioned in art. 9,
    - the transfer is made for the purposes of demonstration, evaluation or exhibition,

  - the transfer is made for the purposes of maintenance and repair, if the recipient is the originating supplier,
  - Member States participate in intergovernmental cooperation programme on development of new products.

  The supplier shall inform Member State of the intention to use the general licence for the first time,

- global licence – for transfer of products to recipients in one or more other Member States (art. 6.1). For each transfer, Member States shall determine the products (or categories of products) and authorized recipients. Global licence is valid for three years and can be renewed (art. 6.2),
- individual licence – for one transfer of a specified quantity of specified products to be transferred in one or several shipments to one recipient in the following cases (art. 7):
  - the request for licence is limited to one transfer,
  - protection of essential security interest of Member State,
  - compliance with international obligations and commitments of Member States,
  - suspicion of not fulfilling the conditions of global licence by the supplier.

The terms, conditions and type of licence for particular products are determined by the Member States (art. 4.4-7). Yet, there can be situations, when Member States can exempt some transfers from the obligation of prior application for a permit in particular cases, e.g. when transfer is related to humanitarian aid or crisis situation, technical service or demonstrations of products (art. 4.2). Also, Member States can block the transfer of products in cases like:

- protection of essential security interests of Member State or public security and as a result of non-compliance with terms and conditions of licence. This may result in withdrawal, suspension or limitation of licence (art. 4.9),
- relevant information was not taken into account when granting licence or since granting of the licence the circumstances has changed significantly. This may result in suspension of transfer process for up to 30 working days (art. 11.2),
- the recipient certified accordingly to art. 9 will not comply with the conditions attached to general licence or the public policy, public security of essential security interests may be affected. This may result in suspension of the effects of particular licence to such recipients (art. 15),
- the recipient is not satisfying the criteria of the certificate of reliability. This may result in revocation of this certificate (art. 9.7).

The certificate, mentioned few times earlier, is document of reliability of the recipient, who shall comply with several criteria (art. 9.2), e.g.:

- proven experience in defence activities, taking into account e.g. compliance with export restrictions, commercialisation of defence-related products, etc.
- appointment of senior executive responsible for transfers and export,

- signing commitment about undertaking steps to enforce specific conditions related to end-use of the product,
- implementation of internal programme or transfer management system.

The certificates can contain information about the terms of their suspension or revocation (art. 9.4). In order to fasten the business activities, Member States shall publish the lists of certified recipients (art. 9.8).

Beside the main obligation of applying for the licence, the Directive mentions some other ones that shall be undertaken by the supplier and the recipient:

- supplier shall inform recipients of the terms and conditions of the licence, including limitations (art. 8.1),
- supplier shall inform Member State, from whose territory the transfer will start, of intention to use a general licence for the first time (art. 8.2),
- supplier shall keep detailed and complete records of the transfers for appropriate period of time (art. 8.3-4),
- recipients of products, when exporting these products, shall inform their authorities, that they are complied with export limitations of the product's country of origin (art. 10),
- supplier shall deliver a proof of having export licence to the customs office (art. 11.1).

Other rules worth mentioning include obligations for the Member States to implement the Directive's regulations into national law (art. 18) along with the penalties for violation of the Directive's regulations, especially those in art. 8.1 and art. 10 (art. 16).

A2.4 Documents concerning security and defence procurement carried out by the Ministry of Defence (in Poland)

Due to the specific purpose of the products, the purchases of equipment for the army are carried out in a strictly defined manner. Based on the "Regulation of the Council of Ministers of 9th July 1996 on detailed scope of operation of Ministry of Defence", in the "Decision of the Minister of Defence no 458/MON of 8 December 2010 on giving detailed scope of operations of the Armament Inspectorate"[37] the Minister of Defence defined the military body, that will be responsible for carried out the procurement processes. Procedures for carrying out purchases are described in other documents, presented below.

The document that describes procurements for MoD in general is the "Decision of the Minister of Defence no 141/MON of 5 July 2017 on the system of acquisition, use and decommissioning of military equipment of the Armed Forces of the Republic of Poland"[38]. Although, it is the set of rules for the military institutions on carrying out particular processes related to the lifecycle of their equipment, some rules indirectly present obligations for the supplier. They are mainly related to delivery of some documents and participation is tests of proposed equipment. Such obligations can occur even before signing the deal – the supplier can be requested to submit its equipment under the verification of critical parameters (§ 69, details in § 70-73), to check if they meet the purchaser's requirements. Later, at the realisation phase of the contract, if the purchase is based on adjustment of the equipment, the supplier may be obliged by the agreement to prepare preliminary design - a subject for an approval (pts 7-8 of Annex 4). Also, new equipment can be put through the set of verification test to check the tactical and technical parameters of the solution. The set of requirements to be tested shall be defined in technical specification (§ 74-77 and pt 13 of Annex 4). This technical specification and other rules of checking products' conformity is described in the "Act of 17 November 2006 on the system of assessing the conformity of products intended for the needs of national defence and security"[39], that will be presented in the further part of this chapter.

In order to rationalize the budget for the conceptual phases of the development of new equipment, § 30 of the Decision allows to exploit the results of national and international research projects or strategic research programmes and development work, even carried of outside MoD, but with MoD's supervision. This allows the MoD to cooperate with external supplier/developers. Annex 3 presents details of the execution of development work and cooperation between MoD and developers. As mentioned in points 11 and 28 of the Annex, some work, such as preparation of the conceptual design or the production of the prototype can be delivered by the supplier chosen accordingly to the law. Sometimes the results of development work with MoD can be a subject to security evaluation, if needed, carried out by the Internal Security Agency and the Military Counterintelligence Service. If the product is

[37] Available at https://archiwum2019-bip.mon.gov.pl/prawo/artykul/dziennik-urzedowy-mon/rok-2010-103246/, PL, access: 14th Dec 2020

[38] Available at http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-149-decyzja-nr-141mon-z-dnia-5-lipca-2017-r-w-sprawie-systemu-pozyskiwania-eksploatacji-i-wycofywania-sprzetu-wojskowego-silzbrojnych-rzeczypo/, PL, access: 14th Dec 2020

[39] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000114, PL, access: 14th Dec 2020

mentioned for the protection of classified information it shall have appropriate certificates, given by governmental agencies (pt 57 of Annex 3). The finish of every stage of the development work (task, workpackage, the end of work) requires the preparation of handover protocol, signed by representatives of the purchaser and supplier. Only the protocol accepted by the chief of armaments inspectorate allows the supplier to prepare the invoice for the purchaser (pt 63 of Annex 3). The final report of the work shall be also prepared. It should contain e.g. description of the results, calculation of costs, list of bought and produced assets, IPR regulations concerning the results, proposition of the management of the assets (pt 64 of Annex 3). Pt 4 of Annex 5 allows for temporary storage of assets at supplier's premises.

In its last paragraphs, the Decision presents the possibility to get familiar with a new equipment provided by the industry (§ 93, details in § 94-96). This is a big opportunity for the suppliers to interest the MoD with their newest creations, despite the fact, that they have to pay for these tests (§ 96).

The supportive document to above Decision is mentioned earlier "Act of 17 November 2006 on the system of assessing the conformity of products intended for the needs of national defence and security". This document describes the processes of the evaluation of the products for military purposes and rules of accreditation and supervision over certification entities. Evaluation can be carried out as (art. 6.1):

- evaluation activities performed by the supplier,
- testing performed by a research institution,
- certification performed by a certification institution.

Besides ammunition, weapons, explosives, vehicles and other typical military equipment, the following products shall be tested (art. 6.2):

- devices for police and military purposes, used for detection and identification of highly toxic chemical substances, biological agents, nuclear weapon as well as their countermeasures,
- devices and measures for individual and collective protection,
- systems, subsystems and components for mentioned equipment.

No matter the type of evaluation activities, it is up to the supplier to organize the whole process. In the simplest case, the supplier performs testing activities and presents the declaration of conformity (art. 7). If the test are to be performed by either research institution or certification institution, it is up to the supplier to select the institution, submit the request for the tests and deliver the equipment along with accompanying documents, e.g. manuals, technical specifications (art. 8-9). Based on the received reports and certificates, the supplier prepares the declaration of conformity (art. 8.12 and 9.12). All documents used for preparation of the declaration of conformity shall be stored by the supplier for 10 years after stopping of the production of the product (art. 13). According to art. 20.3 the product cannot be used without the declaration, that the product is as declared, based on granting the supplier a positive assessment of conformity (art. 18) and other control activities, that may include monitoring and evaluation of processes carried out by the supplier as well as evaluation of the supplier's quality management system for conformity with appropriate international standards or NATO's requirements – for the delivery of a mass product (art. 19). All tests at research or certification institutions are paid by the supplier (art. 26).

Documents described above present the MoD procurement procedures in general. Yet, there are cases, that shall be carried out in a different way. According to the article 346 of the "Treaty on the Functioning of the European Union", Member State may take appropriate measures to ensure the protection of the essential security interests when the case is connected with the production or trade of arms, ammunition and war material. Thus, some purchases for the armed forces can be exempt from the path of public procurement and then can be carried out accordingly to the procedures announced by the Ministry of Defence.

In Poland, such cases are regulated by the "Regulation of the Council of Ministers of 12 February 2013 on the procedure to be followed in assessing the existence of an essential security interest"[40]. This document present the guidelines for the purchaser, that have to be followed during preparation of the request of the assessment of the existence of an essential security interest. Such request shall include (§ 4.1.2):

- pointing out the particular security interest,
- a cause-and-effect premise connecting the product and the security interest,
- explanation, that such procedure won't have negative impact on the competitiveness on internal market in relation to products, that are not mentioned for military purposes.

The assessment is to be done in 30-day-period by appropriate Minister (supervisor of the purchaser) or central government administration body (self-procurement) (§ 5).
The assessment and required request are related to defence area, for which Ministry of Defence is responsible. Thus, the preparation of the requests lies in MoD's competencies. Detailed instruction on preparation of the request is presented in the "Decision of the Minister of Defence no 92/MON of 21 March 2014 on the detailed procedure for the qualification of contracts and assessment of the existence of the basic state security interest"[41]. Despite the necessity to include the description of so-far suppliers or supply chain (pt 3.6.c), the Decision doesn't imply any burdens for these (or future) suppliers.

The details of procurements exempted from public proceeding are presented in the "Decision of the Minister of Defence no 367/MON of 14 September 2015 on the rules and mode of granting contracts at the MoD regarding essential security interests of the state"[42]. The document describes procedures of purchasing equipment; some of them imply various obligations for supplier. Due to the necessity of protection of security interest of the State, the supplier has to meet several requirements, related to protection of classified information. If the supplier is a foreign institution its permissions and certificates have to be checked by

[40] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20130000233, PL, access: 14th Dec 2020

[41] Available at http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-101-decyzja-nr-92mon-z-dnia-21-marca-2014-r-w-sprawie-szczegolowego-trybu-postepowania-w-zakresie-kwalifikacji-zamowien-i-oceny-wystepowania-p/, PL, access: 14th Dec 2020

[42] Available at http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-265-decyzja-nr-367mon-z-dnia-14-wrzesnia-2015-r-w-sprawie-zasad-i-trybu-udzielania-w-resorcie-obrony-narodowej-zamowien-o-podstawowym-znaczeni/, PL, access: 14th Dec 2020

Internal Security Agency in cooperation with Military Counterintelligence Service (§ 10.6.1.h). If at any stage of procurement the classified information is shared, the supplier has to deliver appropriate certificates (§ 19.1.1.c). Also, concession or licence or permit are required for particular products or types of products (§ 19.1.1.b). As the subcontracting is allowed when agreed with the purchaser, the subcontractors have to fulfil the same safety requirements as the supplier (§ 17-18).

Another important rules may imply delivery of some documents/information by the supplier on demand of the purchaser during procurement preparation phase. Some of these documents are:

- information about supplier's experience: list of previous contracts from the last 5 years, including: prices, products, dates of deliveries and receiving parties (§ 19.1.2.a),
- information about quality of production: documents confirming the implementation of quality management systems, in particular NATO AQAP 2000 contract series type (§ 19.1.3.c),
- financial information: financial report for the last 3 years, bank's information about the possessed financial resources or credits, the proof of having liability insurance (§ 19.1.5),
- technical information: documents or samples or declarations about the fulfilling of the requirements by offered goods or services (§ 19.6).

Depending on the number of offers meeting the requirements of protection of essential security interest, the purchaser can choose the type of purchase – negotiations with one or multiple suppliers (§ 25.1 and § 26.1). In case of negotiations with multiple suppliers, the purchaser can introduce a necessity of submission of deposit in the amount of 0,5-3% estimated contract value (§ 28.1 and 28.3). In justified cases (but they are not presented), the purchaser can select only one supplier for further negotiations (§ 25.21). § 30 presents the rules of excluding of suppliers, who had previously been in conflict with law in the past.

Another document that regulates the procurement processes, exempt from public proceeding based on art. 346 of TFEU is the "Act of 26 June 2014 on some agreements concluded in connection with the implementation of product orders with essential importance to state security"[43]. According to art. 7.4 of the Act it is necessary to justify the offset with the protection of the essential security interest. The Act presents rights and obligations for both parties of the agreements (State Treasury and a foreign supplier) for delivery of products, which implementation requires the offset (art. 1). The offset is described as transfer of the technology or know-how together with intellectual property rights, enabling the State Treasury to be independent from the foreign supplier (art. 2.2). The receiver of offset in Poland can be a company mentioned in art. 7.1 of the "Act of 13 June 2019 on conducting business activities in the field of production and trade of explosives, weapons, ammunition as well as products and technology for military or police purposes" (art. 2.4) – it shall have a concession for trading of certain products. Neither of parties can withdraw from

[43] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20140000932, PL, access: 14th Dec 2020

the offset agreement (art. 3.2). The offset agreement is made after the negotiations with a foreign supplier after presenting an offer in Polish language (art. 7.1 and art. 12.1). The foreign supplier shall submit the offset offer to the MoD not later than the delivery offer to a purchaser (art. 8.5). If the supplier's delivery offer is selected by the purchaser (rating includes the rating of the offset offer), the Minister of Defence starts the negotiations on the offset offer (art. 8.6-8). The MoD can reject the proposition of the offset offer and continue the process with the another offset offer, which delivery equivalent has been highly ranked by the purchaser (art. 8.12-13). Upon signing the offset agreement, the foreign supplier shall deliver a financial proof of securing the proper implementation of the offset agreement (art. 20).

The foreign supplier implementing the offset agreement is obliged to submit a report on the realisation of the agreement annually at the end of the first quarter or at any request of the MoD (art. 16). MoD can carry out the control of the correctness of the implementation of offset obligations by the purchaser (art. 17.1). The foreign supplier is also warned of the potential financial penalties for failure in fulfilling the offset obligations (art. 23.2-5) .

A2.5 Documents concerning Internal Control System

Some products for security and defence, their elements, related technologies and chemical substances can be classified as dual-use products. Due to the importance of such products, a set of procedures concerning export, transfer, brokering and transit of dual-use products has been introduced by the "Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items"[44]. Export is recognized by art. 161 of the "Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code" – consolidated version[45] as transfer of products beyond customs area of UE, **transit is recognized as transfer of products from and to non-EU country through customs area of EU**. This set of procedures is called Internal Control System.

According to the definition from the Regulation:

> *'dual-use items' shall mean items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.*

The Regulation lists these products in the Annex I. The Regulation have been modified multiple times by other documents since its publishing in 2009. The list of products was updated in 2019 by the "Commission delegated regulation (EU) 2019/2199 of 17 October 2019 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items"[46]. This was possible according to art. 15.1, saying that list of dual-use products can be updated, based on obligations of the Member States.

[44] Available at https://eur-lex.europa.eu/eli/reg/2009/428/2019-12-31, multiple languages, access: 14th Dec 2020
[45] Available at http://data.europa.eu/eli/reg/1992/2913/2014-01-01, multiple languages, access: 14th Dec 2020
[46] Available at https://eur-lex.europa.eu/eli/reg_del/2019/2199/oj, multiple languages, access: 14th Dec 2020

The Regulation introduced various kinds of permit, which is a document granted by the local authorities for a contractor willing to relocate the products. Exporters are obliged to keep records of their export and brokerage transactions (art. 20). A permit is required for export and brokerage of the dual-use products, mentioned in Annex I (art. 3.1, 4.1 and 5.1), but it may also be required for export, brokerage and transit of some dual-use products not mentioned in Annex I (art. 4.2, 4.3, 5.2 and 6.3). The template of the international general permit for some types of export was introduced in Annex II (art. 9.1) and other types of permit are granted by authorities from country of contractor's residence (art. 9.2). Applications for transfer permit should be submitted in the country from which dual-use products will be sent (art. 23.3). A permit is to be shown to customs office (art. 16.1). All types of permits are valid within EU (art. 9.2), but national general permit is not valid for some products (art. 9.4.a and 9.4.c).

The Regulation also warns, that in some cases due to security reasons transit or export of dual-use products may be prohibited (art. 6.1 and art. 8), once granted permit can be made invalid, suspended, modified or revoked (art. 13.1) and some situations may cause suspending of the export of certain dual-use products for a period of time (art. 16.3).

Besides the Regulation 428/2009, additional – national rules – may apply. Polish "Announcement of the Marshal of the Sejm of the Republic of Poland of 25 April 2019 on the publication of the uniform text of the Act on foreign trade in goods, technologies and services of strategic importance for state security, as well as for the maintenance of international peace and security"[47] implements general rules from Regulation 248/2009, but add some rules concerning other types of products, that are essential to the security interest of the country.

The Act specifies that a permission is not necessary for import or intra-EU transit within Poland (art. 6c), but is required in some cases for technical support for dual-use products (art. 6.1) and for trade of armament (art. 6a.1). The other rules concerning permits states that:

- when applying for a permit with supporting documents in foreign languages, it is necessary to attach their translation made by sworn translator (art. 9.7),
- when applying for a permit for trading weapons or using such permit it is obliged to create and use internal system for control and managing of trading weapons called "internal control system" (art. 11),
- permits have expiry date (art. 14.5).

The Act introduces various certificates, granted for import or export purposes. First of them is import certificate, which is prepared by trade control authority when it is needed by a foreign exporter's national authorities. National trade control authority can also certify the end user statement (art. 22.1). In reverse situation (export) Polish trade control authority requires the delivery of import certificate or end user statement from foreign importer or end-user for export or intra-EU transit purposes (art. 23.1). The necessity of having other type of

[47] Available at http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000953/U/D20190953Lj.pdf, PL, access: 14th Dec 2020, new version: at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000509, PL, access: 14th Dec 2020

certificate appears when the importer has received its products. Then it has to apply for certificate of delivery validation, stating that the delivery took place in accordance with the law (art. 24.1). The last certificate is related to import of armament based on general permits for intra-EU transfer, granted by other Member States' agencies. Upon request of foreign agencies, the importer applies to Internal Security Agency for a certificate of credibility (art. 21e). Other rules introduce some paperwork: when trading goods of strategic importance, it is necessary to keep records of the trades (art. 25.1) and when exporting and trading goods, it is necessary to prepare occasional reports about the execution of the trades (art. 26.1 and 27a). The Act also warns, that trading against the law is a subject to punishment in form of prison or fine (art. 33 - 39).

There is also the "Regulation of the Prime Minister of 8 May 2014 on the template of the notification of the intention to import or intra-EU transfer of dual-use items used in telecommunications or for information security"[48], which introduces the template of the notification.

[48] Available at http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20140000623/O/D20140623.pdf, PL, access: 15th Dec 2020

A2.6 Documents concerning classified information

In some cases, trade of special products is connected with processing of classified information. Such information can be processed by the employees having personnel clearances in dedicated facilities with clearances. In Poland, rules on granting these clearances are presented in the document concerning the protection of classified information. It's newest edition has been published as the "*Announcement of the Marshal of the Sejm of the Republic of Poland of 15 March 2019 on the publication of the uniform text of the Act on the protection of classified information"*[49].

The Act describes what types of information have to be classified and who classifies them (chapter 2). Protection of classified information is supervised by the Internal Security Agency which roles and mandates are described in art. 10, art. 11 and art. 12. Art. 13 presents the duties of the head of the institution, which processes classified information. There should be specially appointed person in the institution – security officer, who is responsible for the compliance with the regulations concerning protection of the classified information(art. 14). The officer's duties are presented in art. 15.

Processing of the classified information can be done by a person who completed training on protection of the classified information and was granted personnel security clearance (art. 21.1). While the training is described in chapter 4, worth pointing out is differentiation of the levels of trainees in the institution, which corresponds with appropriate level of trainers (19.2), and burdening the institution with training costs (art. 19.4). Granting a personnel security clearance is based on the results of the screening (or extended screening), the details of which are described in art. 22-26. It is worth mentioning, that the candidate shall fill the questionnaire, which include many questions concerning some aspects of private life. The questionnaire is the Annex to the Act (art. 24.10). Granted clearances have expiration date (art. 29.3). If needed, the validity of the clearances can be extended when applied by the head of the institution at least 6 month before expiration date of the valid clearance (art. 32.1). In case of refusal or cancellation of personnel security clearance or discontinuation of the screening by national security agencies, one can appeal to the Prime Minister (art. 35.1) not later than 14 days after receiving the decision (art. 35.2).The appeal is being considered not longer than 3 months after its submission (art. 35.4). The same conditions apply for an appeal concerning refusals made by institution's security officer (art. 37.1). One can submit a complaint on the decision of the appeal body to administrative court not later than 30 days after receiving the decision (art. 38.1).

When in the institution there is a processing of information at "secret" or "top-secret" classification level, the head must introduce a special unit called confidential office as a separate organisational division in the institution (art. 42.1), in which the processing may take place. When processing is carried out using IT systems, they have to be accredited by national

[49] Available at http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000742, PL, access: 17th Dec 2020

security agency for “confidential” and above classification level information (art. 48.1 and art. 48.3) or the head of the institution for lower than “confidential” classification level information (art. 48.9). The application for accreditation is usually considered up to 6 months, but in difficult cases this period can be extended for another 6 months (art. 48.4). When granted, accreditation is valid for 5 years (art. 48.2). The appeal is not possible on refusal of granting the accreditation. Means for the electromagnetic protection of “confidential” and above classification level information as well as hardware and software for data encryption shall be tested and certified by national security agency (art. 50.1-3). The appeal is not possible on refusal of granting the certificate (art. 50.4). Both certification and accreditation processes are to be paid by the institution (art. 53.1). Personnel responsible for the protection of classified information in order to perform their duties shall be trained (art. 52.4) and cost of the training is burdening the institution (art. 52.5).

The institution may process “confidential” and above classification level information only when granted facility clearance – a proof of capability to protect such information (art. 54.1-2 and art. 54.9). Clearance has expiration date related to the level of the classified information to be processed (art. 55.2). Clearance is granted after the screening of the company and particular employees (art. 57), which may take up to 6 months (art. 59). Screening is paid by the screened institution (art. 61.1). The appeal to the Prime Minister or complaint to administrative court can be submitted after the refusal of granting the facility clearance (art. 67.2 and art. 69).

Institution signing the agreement concerning the access to “confidential” and above classification level information, shall inform national security agency of the details of such agreement (art. 71.5).

A3 Conclusions

Security and defence procurement is regulated with a set of rules, related mainly to public or national security and prevention from unauthorized use of such equipment. A part of the rules implies a number of obligations to be fulfilled by the purchaser, but there are many obligation for the provider of technology, products and services.

First of all, the supplier has to be acknowledged with a set of documents – not only those related to conducting business activities. Depending on the kind of the end-user (civil agencies of armed forces) or traded product (e.g. involving access to classified information) there is a number of additional documents to get familiar with, which have multiple cross-references or references to other documents, related to the areas beyond security and defence. This creates a complex environment when trading a product, that can be a subject to various rules from different areas (for example: trading of a CWA detector being integrated into bigger system could be connected with concession, internal control system, classified information and military rules on trading equipment). As the general sets of instructions for the conducting business are available (but still don’t contain all the information), there is a lack of such mentioned for security and defence procurement. A list or manual, consisting of the references to the necessary documents (the newest available would be the best), would be very helpful to be in touch with the law. This is particularly important for new companies, that don’t have enough manpower or experience to find and analyse all necessary documents. It would be optimal, that this list/manual was created and maintained by a governmental agency in order to provide and protect its integrity and reliability. Another problem, that should be solved is the need to monitor the changes, that are being introduced to particular documents by legal processes. Such updates often reference or even change additional documents related to the topic. Due to the fact that security and defence procurement require knowledge of numerous documents, tracking their changes is very hard and the supplier needs to look for changes by himself. If there was a complied information on the topic (e.g. mentioned earlier list of documents or a manual) it would be easier and faster to find necessary information.

Another big step for the supplier is implementation of organisational changes in the company. They are connected with various aspects of the business and come mainly from the rules on concession and classified information. The supplier have to prepare its organisational structure and individual employees to fully meet the rules. The company should employ people on special positions, that will be responsible for the compliance with various rules. Another group of employees has to have personnel clearances, if they are dealing with classified information. This may be a problem, as the questionnaires, needed for the application for a clearance, include questions on many aspects of employee’s private life. Thus, some of them may refuse to fill it and ,in the result, they would not be involved in processes, that require access to classified information. Also, all of the employees involved directly into the lifecycle of the special product, even for a small period of time, shall pass the trainings and be legally cleared to work with such technologies. This implies the need to allocate time and money. As for the infrastructure, if the supplier produces or is a physical broker of the special products, in the company there should be specially prepared facilities, designated for production or storage purposes. They have to have appropriate physical dimensions as well as security measurements. For processing of classified information, another specially secured facilities have to be prepared and maintained. The last type of organisational changes are improvements in procedures and supportive documents related to production and quality control. Introduction of such control system is necessary during application for deliveries to the armed forces. Also, rules of concession and internal control system require establishment of the registries of carried out trades and flow of the special products. Introduction of above mentioned improvement is definitely time and money consuming. Rationalisation of this could be a gradient of requirements to be fulfilled. There are some obligations, that can be limited, depending, for example, on the volume or nature of traded goods.

Preparation or acquisition of necessary documents and obligation to provide several information for the authorities is another huge type of the obligations. Documents related to concession, transfer and storage of products, end-users, usage of permits, occasional reports about carried out trades, etc. are additional things about which the supplier has to remember. As the process of granting a particular permit or document by the authorities can take a while, it is necessary to submit the application in advance with a reasonable amount of time. Also, the supplier should wait for the documents from its business partners, that are needed to fulfil the requirements of Internal Control System. In case of sudden business opportunity, there can be problems to trade or transfer a product, because of the lack of required documents. Many documents should be stored for a period of time, so special registers and means to keep them safe need to be introduced in the company. As the supervision of the flow of special products is important from a perspective of agencies responsible for security of society and the State, some obligations, mainly those implying reporting could be limited – similarly to organisational changes, that shall be introduced in company – in order to be related with volume or type of the special product that is being produced/stored/transferred by the supplier. There is also a problem of providing huge amount of various documents, so young company could have a problem of making a complete set or provide some kind of documents (e.g. proving supplier’s experience for purchases run by MoD).

Above mentioned requirements – documents, external validations and tests, special rooms and security measurements, trainings, registers, permissions – require an allocation of the specified amount of time and money. They shall be provided by the supplier, obviously, but it is an investment for a long period of time. On the other hand, the cost of fulfilling of all these obligations is included in the price of the technology, product or service, that is to be paid by the end-user (or the funding institution), financed from the State Treasury. Thus, rationalisation of some rules and requirements would result not only in smaller amount to pay by the purchaser, but also in savings, that could be made by simplification or limitation of supervision processes over some kinds or volumes of special products. These measures could decrease the amount of the public money being spent.

A4 Bibliography

1. Act of 13 June 2019 on conducting business activities in the field of production and trade of explosives, weapons, ammunition as well as products and technology for military or police purposes

2. Act of 17 November 2006 on the system of assessing the conformity of products intended for the needs of national defence and security

3. Act of 26 June 2014 on some agreements concluded in connection with the implementation of product orders with essential importance to state security

4. Act of 29 January 2004 – Public Procurement Law

5. Announcement of the Marshal of the Sejm of the Republic of Poland of 25 April 2019 on the publication of the uniform text of the Act on foreign trade in goods, technologies and services of strategic importance for state security, as well as for the maintenance of international peace and security

6. *Announcement of the Marshal of the Sejm of the Republic of Poland of 15 March 2019 on the publication of the uniform text of the Act on the protection of classified information*

7. Commission Delegated Regulation (EU) 2019/1830 of 30 October 2019 amending Directive 2009/81/EC of the European Parliament and of the Council in respect of the thresholds for supply, service and works contracts

8. Commission Delegated Regulation (EU) 2019/2199 of 17 October 2019 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

9. Common Military List of the European Union

10. Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

11. Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code

12. Decision of the Minister of Defence no 92/MON of 21 March 2014 on the detailed procedure for the qualification of contracts and assessment of the existence of the basic state security interest

13. Decision of the Minister of Defence no 141/MON of 5 July 2017 on the system of acquisition, use and decommissioning of military equipment of the Armed Forces of the Republic of Poland

14. Decision of the Minister of Defence no 367/MON of 14 September 2015 on the rules and mode of granting contracts at the MoD regarding essential security interests of the state

15. Decision of the Minister of Defence no 458/MON of 8 December 2010 on giving detailed scope of operations of the Armament Inspectorate

16. Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community

17. Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC

18. Regulation of the Council of Ministers of 12 February 2013 on the procedure to be followed in assessing the existence of an essential security interest

19. Regulation of the Council of Ministers of 17 September 2019 on classification of types of explosives, weapons, ammunition and products and technologies for military or police purposes, the production or trade of which requires a concession

20. Regulation of the Minister of Economy of 25 September 2002 on training confirming professional preparation to perform or manage a business in the field of manufacturing and trading in explosives, weapons, ammunition and products for military or police purposes, and trading in technology for this purpose

21. Regulation of the Minister of Economy of 27 October 2010 on storage rooms and facilities for the storage of explosives, weapons, ammunition and products for military or police purposes

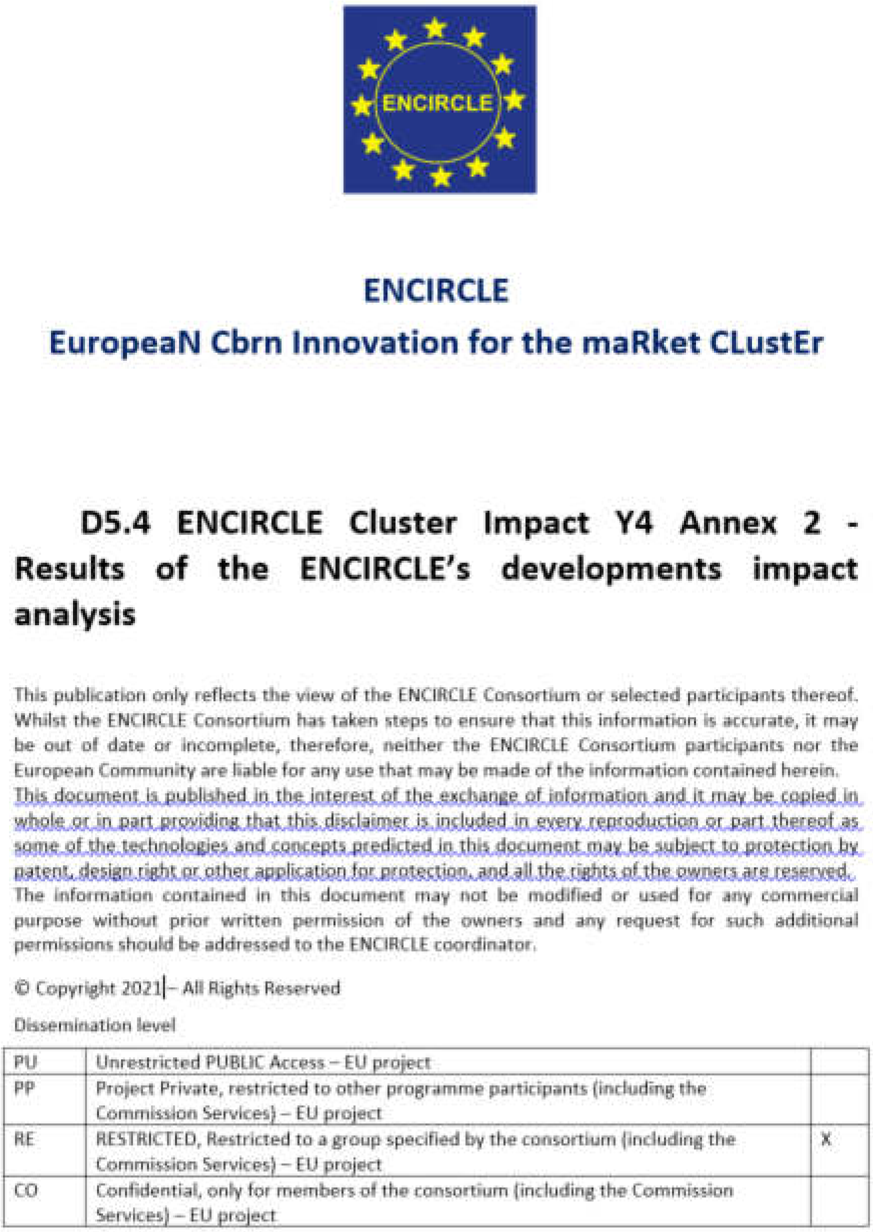
22. Regulation of the Minister of the Interior and Administration of October 30, 2019 on the recording of explosives, weapons, ammunition, products and technologies for military or police purposes as well as trade and brokerage transactions intended for trading and accepted for storage or in commissioning

23. Regulation of the Prime Minister of 8 May 2014 on the template of the notification of the intention to import or intra-EU transfer of dual-use items used in telecommunications or for information security

24. Treaty on the Functioning of the European Union

5 ANNEX 2 ENCIRCLE CLUSTER IMPACT

This report is restricted to a group specified by the consortium (including commission services)



ENCIRCLE

ENCIRCLE

EuropeaN Cbrn Innovation for the maRket CLustEr

D5.4 ENCIRCLE Cluster Impact Y4 Annex 2 - Results of the ENCIRCLE's developments impact analysis

This publication only reflects the view of the ENCIRCLE Consortium or selected participants thereof. Whilst the ENCIRCLE Consortium has taken steps to ensure that this information is accurate, it may be out of date or incomplete, therefore, neither the ENCIRCLE Consortium participants nor the European Community are liable for any use that may be made of the information contained herein. This document is published in the interest of the exchange of information and it may be copied in whole or in part providing that this disclaimer is included in every reproduction or part thereof as some of the technologies and concepts predicted in this document may be subject to protection by patent, design right or other application for protection, and all the rights of the owners are reserved. The information contained in this document may not be modified or used for any commercial purpose without prior written permission of the owners and any request for such additional permissions should be addressed to the ENCIRCLE coordinator.

Dissemination level

PU	Unrestricted PUBLIC Access – EU project	
PP	Project Private, restricted to other programme participants (including the Commission Services) – EU project	
RE	RESTRICTED, Restricted to a group specified by the consortium (including the Commission Services) – EU project	X
CO	Confidential, only for members of the consortium (including the Commission Services) – EU project	